

JP1 Version 13

**JP1/Automatic Job Management System 3 for
Cloud Service Applications**

3021-3-L61-10(E)

Notices

■ Relevant program products

For details about the applicable OS versions, and the service packs and patches required for JP1/Automatic Job Management System 3, see the Release Notes.

JP1/Automatic Job Management System 3 for Cloud Service Applications (For Windows):

P-2A12-3HDL JP1/Automatic Job Management System 3 for Cloud Service Applications 13-10

The above product includes the following:

P-CC2A12-4HDL JP1/Automatic Job Management System 3 for Cloud Service Applications version 13-10 (For Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC2A2C-6LDL JP1/Base version 13-10 (For Windows Server 2022, Windows Server 2019, Windows Server 2016)

JP1/Automatic Job Management System 3 for Cloud Service Applications (For Linux):

P-8412-3HDL JP1/Automatic Job Management System 3 for Cloud Service Applications 13-10

The above product includes the following:

P-CC8412-4HDL JP1/Automatic Job Management System 3 for Cloud Service Applications version 13-10 (For Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

P-CC842C-6LDL JP1/Base version 13-10 (For Linux 7, Linux 8, Linux 9, Oracle Linux 7, Oracle Linux 8, Oracle Linux 9, SUSE Linux 12, SUSE Linux 15)

■ Export restrictions

If you export this product, please check all restrictions (for example, Japan's Foreign Exchange and Foreign Trade Law, and USA export control laws and regulations), and carry out all required procedures.

If you require more information or clarification, please contact your Hitachi sales representative.

■ Trademarks

HITACHI, JP1, Job Management Partner 1, uCosminexus, HiRDB are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)
4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

```
/* =====
```

```
* Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.
```

```
*
```

```
* Redistribution and use in source and binary forms, with or without
```

```
* modification, are permitted provided that the following conditions
```

```
* are met:
```

```
*
```

```
* 1. Redistributions of source code must retain the above copyright
```

```
* notice, this list of conditions and the following disclaimer.
```

```
*
```

```
* 2. Redistributions in binary form must reproduce the above copyright
```

```
* notice, this list of conditions and the following disclaimer in
```

```
* the documentation and/or other materials provided with the
```

```
* distribution.
```

```
*
```

```
* 3. All advertising materials mentioning features or use of this
```

```
* software must display the following acknowledgment:
```

```
* "This product includes software developed by the OpenSSL Project
```

```
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
```

```
*
```

```
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
```

```
* endorse or promote products derived from this software without
```

```
* prior written permission. For written permission, please contact
```

```
* openssl-core@openssl.org.
```

```
*
```

```
* 5. Products derived from this software may not be called "OpenSSL"
```

```
* nor may "OpenSSL" appear in their names without prior written
```

```
* permission of the OpenSSL Project.
```

```
*
```

```
* 6. Redistributions of any form whatsoever must retain the following
```

```
* acknowledgment:
```

```

* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be
given attribution

```

```

* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by Andy Clark.

This product includes the OpenSSL library.

The OpenSSL library is licensed under Apache License, Version 2.0.

<https://www.apache.org/licenses/LICENSE-2.0>

Java is a registered trademark of Oracle and/or its affiliates.



■ Microsoft product screen shots

Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Windows 10	Windows 10(x86)	Windows(R) 10 Enterprise (32bit)
		Windows(R) 10 Home (32bit)
		Windows(R) 10 Pro (32bit)
	Windows 10(x64)	Windows(R) 10 Enterprise (64bit)
		Windows(R) 10 Home (64bit)
		Windows(R) 10 Pro (64bit)
Windows 11	Windows(R) 11 Enterprise (64bit)	
	Windows(R) 11 Home (64bit)	
	Windows(R) 11 Pro (64bit)	
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter	

Abbreviation	Full name or meaning
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
	Microsoft(R) Windows Server(R) 2019 Standard
Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter
	Microsoft(R) Windows Server(R) 2022 Standard

Note:

Windows is sometimes used generically, referring to Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 11, and Windows 10.

■ **Issued**

Sep. 2024: 3021-3-L61-10(E)

■ **Copyright**

Copyright (C) 2023, 2024, Hitachi, Ltd.

Copyright (C) 2023, 2024, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-L61-10(E)) and product changes related to this manual.

Changes	Location
Service linkage monitoring jobs and service linkage objects monitoring jobs were added.	<i>1.1.1, 1.1.2, 2.1.1, 2.2, 2.2.1, 2.2.2, 3.1.1, 3.1.2, 3.1.3, 3.3.1, 3.3.2(1), 3.3.2(2), 3.3.4, 3.3.5, 3.4.1(4), 3.4.1(5), 3.4.1(6), 3.5.1, 3.5.1(3), 3.5.1(5), 3.5.1(6), 3.7.3, 3.8, 4.1.1, 4.1.3, 4.1.5, 4.2, 4.3.1, 4.3.2, 4.3.4, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.6, 5.1, 6., 7., 8. ajscsajobreg (Windows only), 8. ajscsajoblist (Windows only), 8. ajscsajobdel (Windows only), 9.2, 9.2.3, 9.2.4, 9.2.7, 9.2.8, 9.5.4, 9.5.6, Appendix A., Appendix D., Appendix E., Appendix E.2, Appendix E.3, Appendix F.1(2), Appendix F.1(3), Appendix G., Appendix J.</i>
Added following messages: KNBB2418-W, KNBB2419-W, KNBB3035-I, KNBB4003-E, KNBB4011-E, KNBB6005-I, KNBB6011-I, KNBB6012-I, KNBB6013-I, KNBB6014-I, KNBB6015-I, KNBB6016-I, KNBB6017-I, KNBB6018-W, KNBB6102-E, KNBB6103-E, KNBB6104-W, KNBB6105-E, KNBB6106-E, KNBB6107-E, KNBB6150-E, KNBB6151-W, KNBB6152-E, KNBB6153-E, KNBB6154-E, KNBB6155-E, KNBB6156-E, KNBB6157-E, KNBB6158-E, KNBB6159-E, KNBB6160-E, KNBB6161-E, KNBB6162-W, KNBB6163-E, KNBB6164-E, KNBB6306-E, KNBB6307-W, KNBB6308-W, KNBB6309-E, KNBB6310-E, KNBB6311-E, KNBB6312-E, KNBB6402-E, KNBB6403-W, KNBB6449-E	<i>10.2.1, 10.3.1</i>
Changed following messages or description of messages: KNBB2402-Q, KNBB2407-Q, KNBB2408-Q, KNBB2409-Q, KNBB2410-Q, KNBB2411-E, KNBB2412-I, KNBB2413-I, KNBB2415-E, KNBB2417-E, KNBB3291-E, KNBB4002-E, KNBB4003-E, KNBB4501-I, KNBB4508-E, KNBB4511-E, KNBB4512-E, KNBB4514-W, KNBB4515-I, KNBB4517-E, KNBB4518-E, KNBB4519-E, KNBB4520-E, KNBB4523-E, KNBB4524-E, KNBB4525-E, KNBB4526-W, KNBB6004-I, KNBB6200-E, KNBB6201-E, KNBB6203-E, KNBB6301-E, KNBB6450-E, KNBB6451-E	<i>10.3.1</i>
Deleted following messages: KNBB2559-E, KNBB2707-E, KNBB3201-E, KNBB3202-E, KNBB3203-E, KNBB3204-E, KNBB3206-E, KNBB3207-E	<i>10.3.1</i>

In addition to the above changes, minor editorial corrections were made.

Preface

This manual describes the functions of JP1/Automatic Job Management System 3 for Cloud Service Applications (abbreviated hereafter to JP1/AJS3 for Cloud Service Applications).

■ Intended readers

This manual is intended for:

- Those who have constructed, are using, or wish to use an automated job operation system by using JP1/AJS, or who have sufficient knowledge to construct and operate a JP1/AJS system, and wish to use JP1/AJS.
- Those who wish to use JP1/AJS and cloud services together.

■ Organization of this manual

This manual is organized as follows:

1. Functional Overview of JP1/AJS3 for Cloud Service Applications

Chapter 1 explains the functional overview of JP1/AJS3 for Cloud Service Applications.

2. System Configuration of JP1/AJS3 for Cloud Service Applications

Chapter 2 explains the system configuration of JP1/AJS3 for Cloud Service Applications.

3. Designing and Building the System

Chapter 3 describes the procedure for installing and setting up JP1/AJS3 for Cloud Service Applications.

4. Designs and definitions of linkage job

Chapter 4 describes the procedure for defining service linkage jobs and service linkage monitoring jobs using JP1/AJS3 for Cloud Service Applications.

5. Management operation of service linkage jobs

Chapter 5 describes a procedure for executing in JP1/AJS3 a service linkage job defined on JP1/AJS3 for Cloud Service Applications.

6. Management operation of service linkage monitoring jobs

Chapter 6 describes a procedure for executing in JP1/AJS3 a service linkage monitoring job defined on JP1/AJS3 for Cloud Service Applications.

7. Operation

Chapter 7 describes GUI operations in JP1/AJS3 for Cloud Service Applications.

8. Commands

Chapter 8 describes the commands that are used for JP1/AJS3 for Cloud Service Applications.

9. Troubleshooting

Chapter 9 describes the procedures for dealing with problems and the data that must be collected.

10. Messages

Chapter 10 describes the messages that are issued by JP1/AJS3 for Cloud Service Applications.

A. Files and Directories

Appendix A lists the files and directories for the JP1/AJS3 for Cloud Service Applications.

B. Limitations

Appendix B describes the limitations for JP1/AJS3 for Cloud Service Applications.

C. Estimation

Appendix C describes about estimating the resources required to operate JP1/AJS3 for Cloud Service Applications.

D. Port number to be set

Appendix D explains the port number to be set and the direction through the firewall.

E. JP1/AJS3 Environment Setting Parameters

Appendix E provides information about a list of environmental setting parameters configured on JP1/AJS3 installed on the host that runs service linkage jobs and service linkage monitoring jobs of JP1/AJS3 for Cloud Service Applications.

F. Service linkage job information definition files

Appendix F explains the files that define the service linkage job information of JP1/AJS3 for Cloud Service Applications.

G. Service linkage monitoring job information definition files

Appendix G explains the files that define the service linkage monitoring job information of JP1/AJS3 for Cloud Service Applications.

H. Version Revisions

Appendix H explains the version revisions.

I. Reference Material for This Manual

Appendix I provides reference materials for readers of this manual.

J. Glossary

Appendix J defines terms used in this manual.

Contents

Notices 2

Summary of amendments 8

Preface 9

1 Functional Overview of JP1/AJS3 for Cloud Service Applications 16

1.1 Overview of JP1/AJS3 for Cloud Service Applications 17

1.1.1 Features of JP1/AJS3 for Cloud Service Applications 17

1.1.2 Functions that JP1/AJS3 for Cloud Service Applications provides 17

2 System Configuration of JP1/AJS3 for Cloud Service Applications 22

2.1 To check operating environment 23

2.1.1 Prerequisite programs 23

2.2 Consider system configuration 24

2.2.1 Use in on-premises environment 24

2.2.2 Use in cloud environment 28

2.2.3 Configuration in cluster system 34

2.2.4 Operation in disaster-recovery configuration 36

3 Designing and Building the System 37

3.1 Installation 38

3.1.1 Installing JP1/Base 38

3.1.2 Installation (for Windows) 38

3.1.3 Installation (for Linux) 39

3.2 Uninstallation 41

3.2.1 For Windows 41

3.2.2 For Linux 41

3.3 Setup 43

3.3.1 Setup for using service linkage jobs and service linkage monitoring jobs 43

3.3.2 Setting up the SSL communication environment 44

3.3.3 Setting up the cluster environment 50

3.3.4 Setting up the execution host for service linkage jobs and service linkage monitoring jobs 52

3.3.5 Changing the settings during operation 54

3.3.6 Setting automatic startup and termination of the JP1/AJS3 for Cloud Service Applications service 56

3.4 Configuration filedetails (JP1/AJS3 for Cloud Service Applications) 58

3.4.1 Details of setting items of the environment setting file (ajs3csaweb.conf) 58

3.4.2 Details on the settings in the HTTP server definition file (httpsd.conf) 70

3.4.3 User property file for J2EE server (usrconf.properties) 74

3.4.4	Option definition file for J2EE server (usrconf.cfg)	76
3.4.5	System property file for server management commands (usrconf.properties)	78
3.5	Configuration file details (JP1/AJS3)	81
3.5.1	Connection configuration file	81
3.6	JP1/AJS3 for Cloud Service Applications database file	86
3.6.1	Details of database files	86
3.7	Backup and recovery	89
3.7.1	the configuration information for JP1/AJS3 for Cloud Service Applications Backing up	89
3.7.2	the configuration information for JP1/AJS3 for Cloud Service Applications Recovering	91
3.7.3	Backing up and recovering the entire system	91
3.8	Notes when running anti-virus software	92

4 Designs and definitions of linkage jobs 94

4.1	Designs of linkage jobs	95
4.1.1	Flow of designing linkage jobs	95
4.1.2	Consideration according to connection-destination services and command execution environments	96
4.1.3	Considering the method for managing authentication information corresponding to the commands to be executed	96
4.1.4	Considering the linkage processing	97
4.1.5	Considering the monitoring processing	98
4.2	Definition flow of a linkage job	101
4.3	Definition items of linkage job information	102
4.3.1	Variables used for the definition of service linkage job information	102
4.3.2	Variables used for the definition of service linkage monitoring job information	103
4.3.3	Escaping a command line for cloud service linkage information	104
4.3.4	Notes on the definitions of linkage job information	105
4.4	How to define linkage jobs	108
4.4.1	Details of the definition of linkage jobs	108
4.4.2	Place where linkage jobs can be defined	108
4.4.3	Definition items of service linkage jobs	109
4.4.4	Definition items of service linkage monitoring jobs	110
4.4.5	Icon of linkage jobs	112
4.4.6	Operation of service linkage jobs	112
4.4.7	Operation of service linkage monitoring jobs	114
4.4.8	Notes on linkage jobs	115
4.5	Unit definition parameters of service linkage jobs	116
4.5.1	Description format of unit definition parameters of service linkage jobs	116
4.5.2	Details of the unit definition parameters of service linkage jobs	116
4.6	Unit definition parameters of service linkage monitoring jobs	118
4.6.1	Description format of unit definition parameters of service linkage monitoring jobs	118
4.6.2	Details of the unit definition parameters of service linkage monitoring jobs	118

5	Management operation of service linkage jobs	121
5.1	Execution of service linkage jobs	122
5.2	Details of service linkage jobs	123
5.2.1	Status of service linkage jobs	123
5.2.2	Environment variables for command execution	123
5.2.3	Execution results of service linkage jobs	123
5.2.4	Killing of service linkage jobs	124
5.2.5	Return codes of service linkage jobs	125
5.3	Notes on execution of service linkage jobs	126
6	Management operation of service linkage monitoring jobs	127
6.1	Types and execution of service linkage monitoring jobs	128
6.2	Details of service linkage objects monitoring jobs	130
6.2.1	Monitoring functions of service linkage objects monitoring jobs	130
6.2.2	Service linkage objects monitoring job execution environment and permissions	134
6.2.3	Behavior when the JP1/AJS3 service is started and stopped	136
6.2.4	Passing information of service linkage objects monitoring jobs	137
6.2.5	Execution results of service linkage objects monitoring jobs	139
6.2.6	Forced termination of service linkage objects monitoring jobs	139
6.2.7	Return codes of service linkage objects monitoring jobs	140
6.2.8	Notes on execution of service linkage objects monitoring jobs	141
7	Operation	143
7.1	Web GUI	144
7.1.1	Web browser settings	144
7.1.2	Window transitions	144
7.1.3	Login window	145
7.1.4	Common display items	146
7.1.5	Home window	146
7.1.6	Service linkage job definition window	148
7.1.7	Service linkage monitoring job definition window	151
7.1.8	Execution definitions window	153
7.1.9	Object monitoring definition window	172
7.1.10	Connection definitions window	179
7.1.11	Authentication definitions window	192
7.1.12	Notes on Web GUI	195
7.2	JP1/AJS3 - View Define Details window	197
7.2.1	Define Details window for service linkage jobs	197
7.2.2	Define Details window for service linkage objects monitoring jobs	197
7.2.3	Notes on Define Details window	199

8	Commands 201
	Command description format 202
	List of commands 204
	ajscsasetup (Windows, Linux) 205
	jajs_csa (Linux only) 209
	jajs_csa_stop (Linux only) 211
	jajs_log (Linux only) 213
	jajs_log.bat (Windows only) 219
	ajscsajobreg (Windows only) 225
	ajscsajoblist (Windows only) 228
	ajscsajobdel (Windows only) 232
9	Troubleshooting 235
9.1	Troubleshooting procedure 236
9.2	Types of log information and storage locations 237
9.2.1	Application Server Common Logs 238
9.2.2	Application Server Logs 239
9.2.3	Application server logs (for executing service linkage monitoring jobs) 239
9.2.4	Server Job Logs 240
9.2.5	Command Log 240
9.2.6	Service Linkage Job Log 240
9.2.7	Service Linkage Monitoring Job Log 241
9.2.8	List of log files and directories 242
9.3	Data to be collected when a problem occurs 250
9.3.1	Data to collect 250
9.4	Collecting data for troubleshooting 254
9.4.1	Details of how to collecting data 254
9.5	Troubleshooting 258
9.5.1	Troubleshooting SSL communications 258
9.5.2	Troubleshooting Web Browser Problems 258
9.5.3	Troubleshooting failures of service linkage jobs and linked cloud services 258
9.5.4	Troubleshooting failures of service linkage monitoring jobs and linked cloud services 261
9.5.5	Troubleshooting for service linkage jobs 262
9.5.6	Troubleshooting failures common to both service linkage jobs and service linkage monitoring jobs 262
10	Messages 263
10.1	JP1/AJS3 for Cloud Service Applications Messages 264
10.1.1	Message format 264
10.1.2	Message ID 264
10.1.3	Format of message explanations 264
10.2	List of output destinations for messages 266
10.2.1	Output destinations of messages beginning with KNBB 266
10.3	List of messages 275

Appendixes 346

A	Files and Directories	347
A.1	In Windows	347
A.2	In Linux	349
B	Limitations	351
C	Estimation	352
D	Port number to be set	353
E	JP1/AJS3 Environment Setting Parameters	354
E.1	Format of the environment setting parameters	354
E.2	List of Environment Setting Parameters	354
E.3	Details of the environment setting parameters	356
F	Service linkage job information definition files	361
F.1	Connection definition file	361
F.2	Execution definition file	368
F.3	Service linkage definition file	376
G	Service linkage monitoring job information definition files	378
G.1	Service linkage objects monitoring definition file	378
G.2	Service linkage monitoring job definition file	382
H	Version Revisions	384
H.1	Revisions in 13-10	384
I	Reference Material for This Manual	385
I.1	Related publications	385
I.2	Conventions: Fonts and symbols	385
I.3	Use of folder names and directory names	386
I.4	Conventions: Abbreviations for product names	386
I.5	Conventions: Acronyms	387
I.6	Conventions: KB, MB, GB, and TB	387
J	Glossary	389

Index 394

1

Functional Overview of JP1/AJS3 for Cloud Service Applications

This chapter explains the functional overview of JP1/AJS3 for Cloud Service Applications.

Also explained are service linkage jobs and service linkage monitoring jobs that can be used as the custom jobs of JP1/AJS3 by being defined to JP1/AJS3 for Cloud Service Applications.

1.1 Overview of JP1/AJS3 for Cloud Service Applications

JP1/AJS3 for Cloud Service Applications is a product that supports linkage between a job that has been shifted to the cloud and is using a cloud service and JP1/AJS3 that executes existing main business operations. It can put together information for linkage with cloud services for central management and/or provide such information as a job that can be used with JP1/AJS3.

1.1.1 Features of JP1/AJS3 for Cloud Service Applications

The features of JP1/AJS3 for Cloud Service Applications are described below:

(1) Managing information linkage with a cloud service as a component

The series of processing necessary for linkage with a cloud service, including authentication, execution, monitoring, and result check, was in the past realized by coding processing with a script. With JP1/AJS3 for Cloud Service Applications, information necessary for connection with a cloud service and authentication, the information necessary for execution of the cloud service, and the information necessary for monitoring the status of the cloud service can be created by low-code development as components on a website screen. In addition, these components are combined as a flow of a series of processing and managed as *service linkage job information* and *service linkage monitoring job information*.

When using a new cloud service or when changing linkage processing due to function addition or specification change at the side of the cloud service, linkage with the cloud service can be realized with new linkage processing content by creating or updating a component, which makes it possible to quickly respond to a change in the business operation.

(2) Realizing the business operation of a cloud service with simple job definition

Service linkage job and service linkage monitoring job information created with JP1/AJS3 for Cloud Service Applications can be used as a custom job or custom event job of JP1/AJS3.

This makes it possible to easily load a business operation using a cloud service to the job net of JP1/AJS3, so that the business operation using the cloud service and on-premises main business operation can be seamlessly executed.

This custom job is called a *service linkage job*, and this custom event job is called a *service linkage monitoring job*.

1.1.2 Functions that JP1/AJS3 for Cloud Service Applications provides

JP1/AJS3 for Cloud Service Applications provides these functions:

- Function to define service linkage job information
- Function to define service linkage monitoring job information
- Function to register service linkage job information as a custom job
- Function to register service linkage monitoring job information as a custom event job
- Function to execute service linkage jobs with JP1/AJS3
- Function to execute service linkage monitoring jobs with JP1/AJS3

The functions that JP1/AJS3 for Cloud Service Applications provides are shown in the figure below.

Figure 1–1: Functions that JP1/AJS3 for Cloud Service Applications provides (for custom jobs)

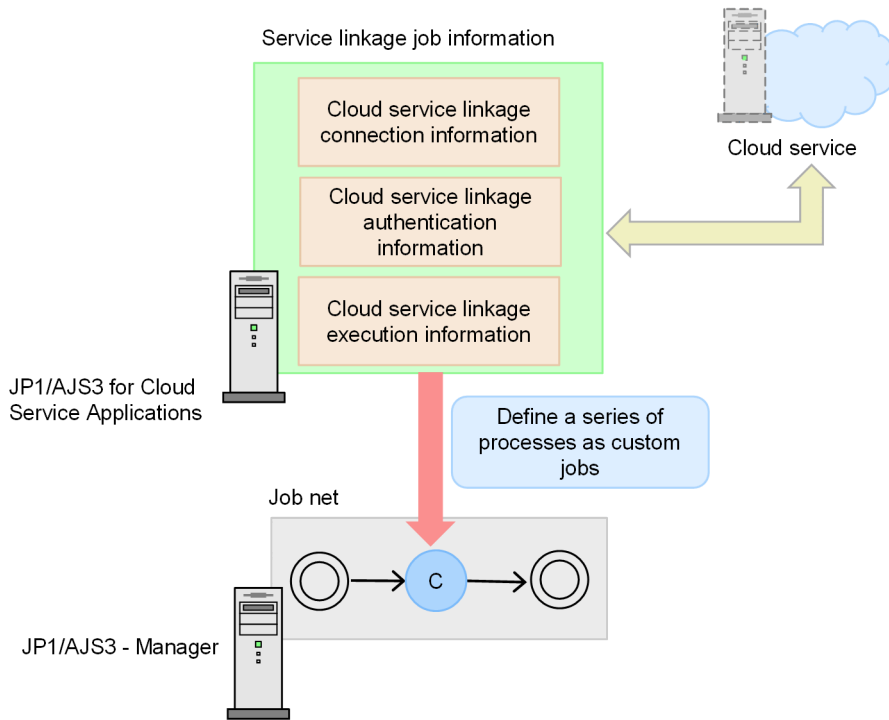
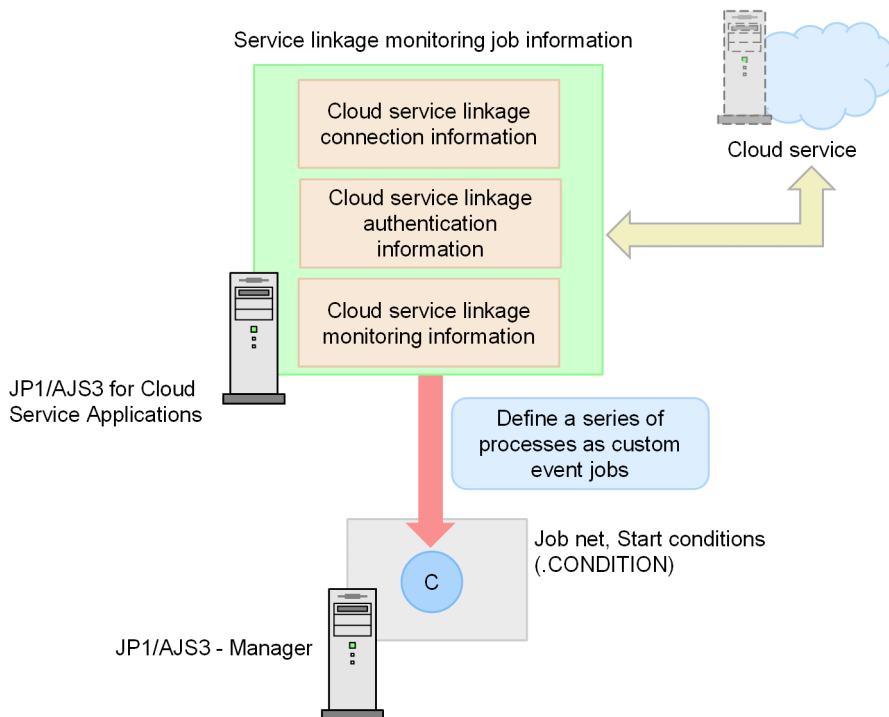


Figure 1–2: Functions that JP1/AJS3 for Cloud Service Applications provides (for custom event jobs)



Tip

This manual may collectively abbreviate service linkage job information and service linkage monitoring job information as *linkage job information*, and service linkage jobs and service linkage monitoring jobs as *linkage jobs*.

(1) Function to define service linkage job information

This function is to define service linkage job information. It is available on the website screen of JP1/AJS3 for Cloud Service Applications.

With JP1/AJS3 for Cloud Service Applications, linkage with a cloud service by using a command line interface (CLI) that can coordinate with the cloud service is assumed. The service linkage job information defines and use this CLI information.

Service linkage job information consists of the following three pieces of information:

Cloud service linkage connection information

This information is on the interface for connecting to the cloud service. For example, the login command and an option for logging in with the user's login information specified as the option fall within this category. This information can be shared with service linkage monitoring job information.

This information is hereafter referred to as *service linkage connection information* or abbreviated as *connection information*. In addition, the definition of service linkage connection information is abbreviated as the *connection definition*.

Cloud service linkage authentication information

This information is necessary for an interface for connecting a cloud service. For example, a username and a password used for authenticating a user account fall under this category. This information can be shared with service linkage monitoring job information.

This information is hereafter referred to as *service linkage authentication information* or abbreviated as *authentication information*. In addition, definition of service linkage authentication information is abbreviated as *authentication definition*.

Cloud service linkage execution information

This is information on an interface for using a cloud service after connection of the cloud service. For example, an execution command and options for executing processing by calling a server-less service, and a result check command and options for checking the result of the processing of the service that was executed fall under this category. This information is hereafter referred to as *service linkage execution information* or abbreviated as *execution information*. In addition, definition of service linkage execution information is abbreviated as *execution definition*.

(2) Function to define service linkage monitoring job information

This function is used to define service linkage monitoring job information. It is available on the Web screen of JP1/AJS3 for Cloud Service Applications.

As with service linkage job information, linkage with a cloud service by using a command line interface (CLI) that can coordinate with the cloud service (enabling the user to verify service status and information over the cloud) is assumed. The service linkage monitoring job information defines and uses this CLI information.

Service linkage monitoring job information consists of the following three pieces of information:

Cloud service linkage connection information

This information is on the interface for connecting to the cloud service. For details, see the description provided for service linkage job information. This information can be shared with service linkage job information.

Cloud service linkage authentication information

This information is necessary for an interface for connecting to a cloud service. For details, see the description provided for service linkage job information. This information can be shared with service linkage job information.

Cloud service linkage monitoring information

This is information on an interface for retrieving and monitoring cloud service status updates and information after connecting to the cloud service. For example, this includes execution commands and options for retrieving file object information from the cloud, and information on the intervals at which the execution results are checked to satisfy monitoring requirements.

This information is hereafter referred to as *service linkage monitoring information* and abbreviated as *monitoring information*. In addition, the definition of service linkage monitoring information is abbreviated as *monitoring definition*.

As the information used as monitoring conditions vary depending on the cloud service being monitored, the abovementioned cloud service linkage monitoring information requires that monitoring information be defined for each cloud service.

The types of monitoring information that can be defined with JP1/AJS3 for Cloud Service Applications are summarized in the table below.

Table 1–1: List of monitoring information that can be defined with JP1/AJS3 for Cloud Service Applications

Name of service being monitored	Name of monitoring information	Description
Object storage service	Cloud service linkage object monitoring information	The interface information for monitoring objects on the cloud. Jobs executed using this information are called <i>service linkage objects monitoring jobs</i> . Hereafter <i>service linkage objects monitoring information</i> , or abbreviated as <i>object monitoring information</i> . In addition, the service linkage object monitoring information definition is abbreviated as <i>object monitoring definition</i> .

(3) Function to register service linkage job information as a custom job

This function registers service linkage job information as a custom job of JP1/AJS3.

By registering service linkage job information defined with JP1/AJS3 for Cloud Service Applications as a custom job from JP1/AJS3 - View, it can be defined as a service linkage job on JP1/AJS3.

(4) Function to register service linkage monitoring job information as a custom event job

This function registers service linkage monitoring job information as a custom event job of JP1/AJS3.

By registering service linkage monitoring job information defined with JP1/AJS3 for Cloud Service Applications as a custom event job from JP1/AJS3 - View, it can be defined as a service linkage monitoring job on JP1/AJS3.

(5) Function to execute service linkage job with JP1/AJS3

This function is to execute a service linkage job with JP1/AJS3.

A service linkage job is executed based on information registered as a custom job and service linkage job information that was obtained from the JP1/AJS3 for Cloud Service Applications server when the job was executed.

(6) Function to execute service linkage monitoring job with JP1/AJS3

This function is to execute a service linkage monitoring job with JP1/AJS3.

A service linkage monitoring job is executed as a custom event job based on information defined for the custom event job, and service linkage monitoring job information that was obtained from the JP1/AJS3 for Cloud Service Applications server when the job was executed.

2

System Configuration of JP1/AJS3 for Cloud Service Applications

This chapter explains the system configuration of JP1/AJS3 for Cloud Service Applications.

2.1 To check operating environment

This section explains the operating environment and prerequisites for JP1/AJS3 for Cloud Service Applications.

2.1.1 Prerequisite programs

The prerequisite programs of JP1/AJS3 for Cloud Service Applications are shown in the following table:

Table 2–1: Prerequisite programs of JP1/AJS3 for Cloud Service Applications

Name of program	Version	Prerequisite
JP1/Base	13-00 or later ^{#1}	In same equipment
JP1/AJS3 - Manager ^{#2}	13-10 or later	In system
JP1/AJS3 - Agent ^{#2#3}	13-10 or later	In system
JP1/AJS3 - View ^{#2}	13-10 or later	In system

#1

13-10 or later versions are prerequisite for using service linkage monitoring jobs.

#2

For the prerequisites of the programs in the JP1/AJS3 series, refer to the description on the prerequisites of JP1/AJS3 in the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*.

#3

Excluding JP1/AJS3 - Agent Minimal Edition

Note that the prerequisite Web browsers for JP1/AJS3 for Cloud Service Applications are shown below. For the supported version, refer to the *Release Note*.

- Microsoft Edge
- Firefox ESR
- Google Chrome

2.2 Consider system configuration

With JP1/AJS3 for Cloud Service Applications, system configuration where an on-premises environment and a cloud environment exist in a mix can be used.

The system configuration of JP1/AJS3 for Cloud Service Applications is shown below.



Note

The system configuration of JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - View is not restricted in any way.

Make sure that the configuration allows connection of service linkage job or the service linkage monitoring job execution destination host (JP1/AJS3 - Agent or JP1/AJS3 - Manager) and JP1/AJS3 for Cloud Service Applications.

2.2.1 Use in on-premises environment

This section describes the system configuration for constructing JP1/AJS3 for Cloud Service Applications in an on-premises environment.

Note that *JP1/AJS3 for Cloud Service Applications* is abbreviated as *JP1/AJS3 for CSA* in the figures of this section.



Note

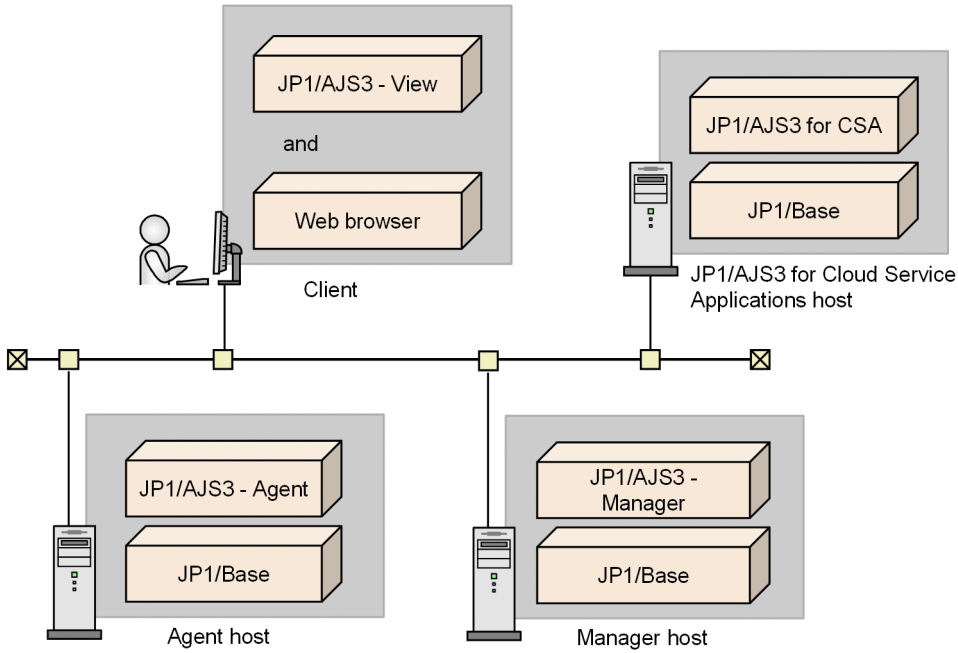
It is also possible to use the manager host as a service linkage job or service linkage monitoring job execution destination host without constructing an agent host.

(1) To construct only JP1/AJS3 for Cloud Service Applications

Construct JP1/AJS3 for Cloud Service Applications in a host separate from the one for JP1/AJS3 - Manager and JP1/AJS3 - Agent.

JP1/AJS3 - Manager and JP1/AJS3 - Agent are constructed in an on-premises environment.

Figure 2–1: Example of system configuration for constructing only JP1/AJS3 for Cloud Service Applications



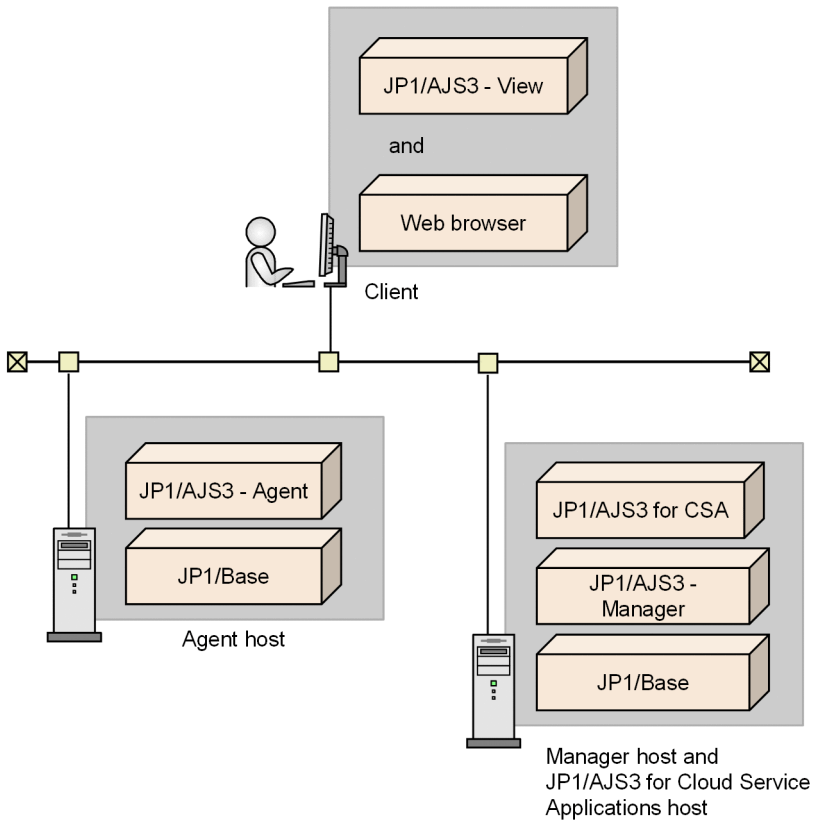
Legend:

JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(2) To construct on-premises JP1/AJS3 - Manager and JP1/AJS3 - Agent in same host

JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - Manager and JP1/AJS3 - Agent are constructed in the same host.

Figure 2–2: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - Manager are on the same host



Legend:

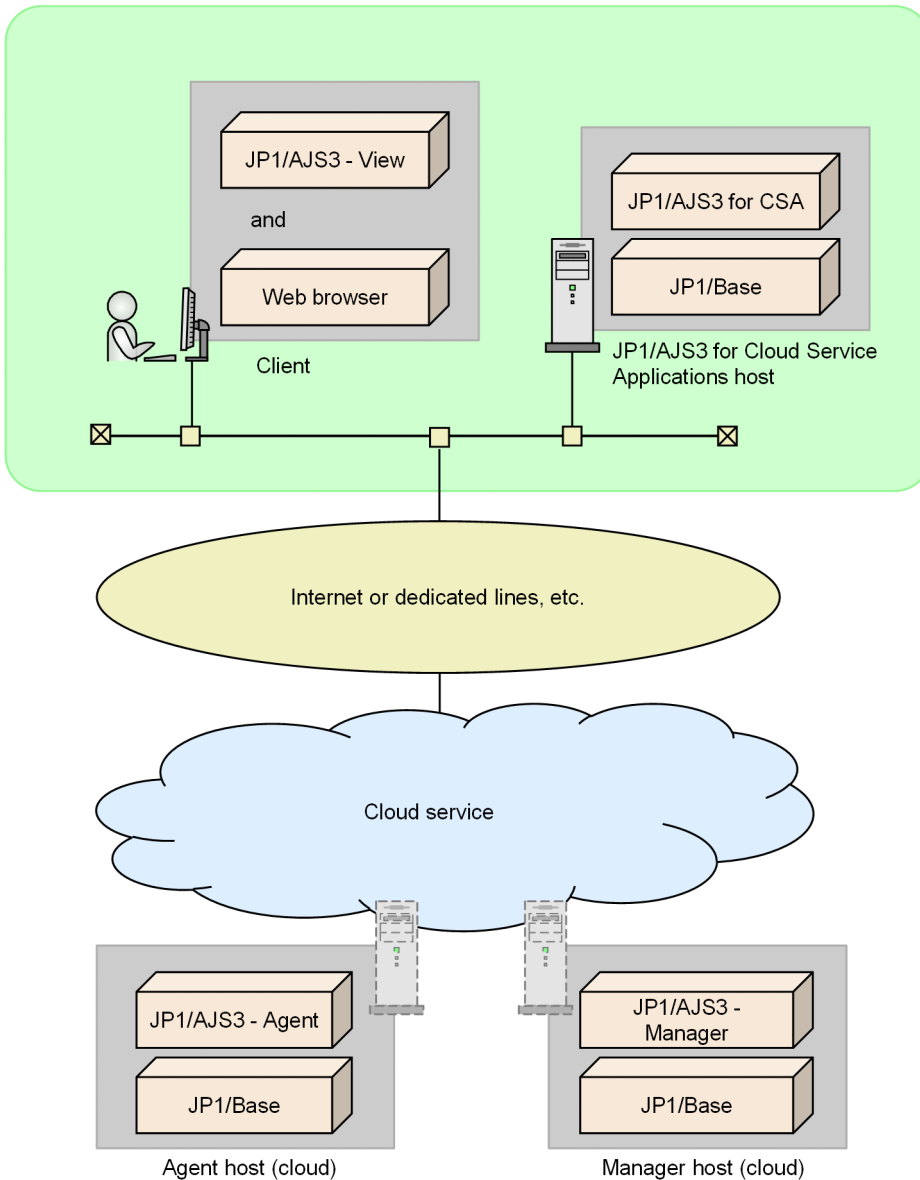
JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(3) To construct JP1/AJS3 - Manager and JP1/AJS3 - Agent in cloud

JP1/AJS3 for Cloud Service Applications is constructed in an on-premises host and JP1/AJS3 - Manager and JP1/AJS3 - Agent are in the cloud.

Figure 2–3: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications in on-premises host and JP1/AJS3 - Manager and JP1/AJS3 - Agent in the cloud

On-premises



Legend:

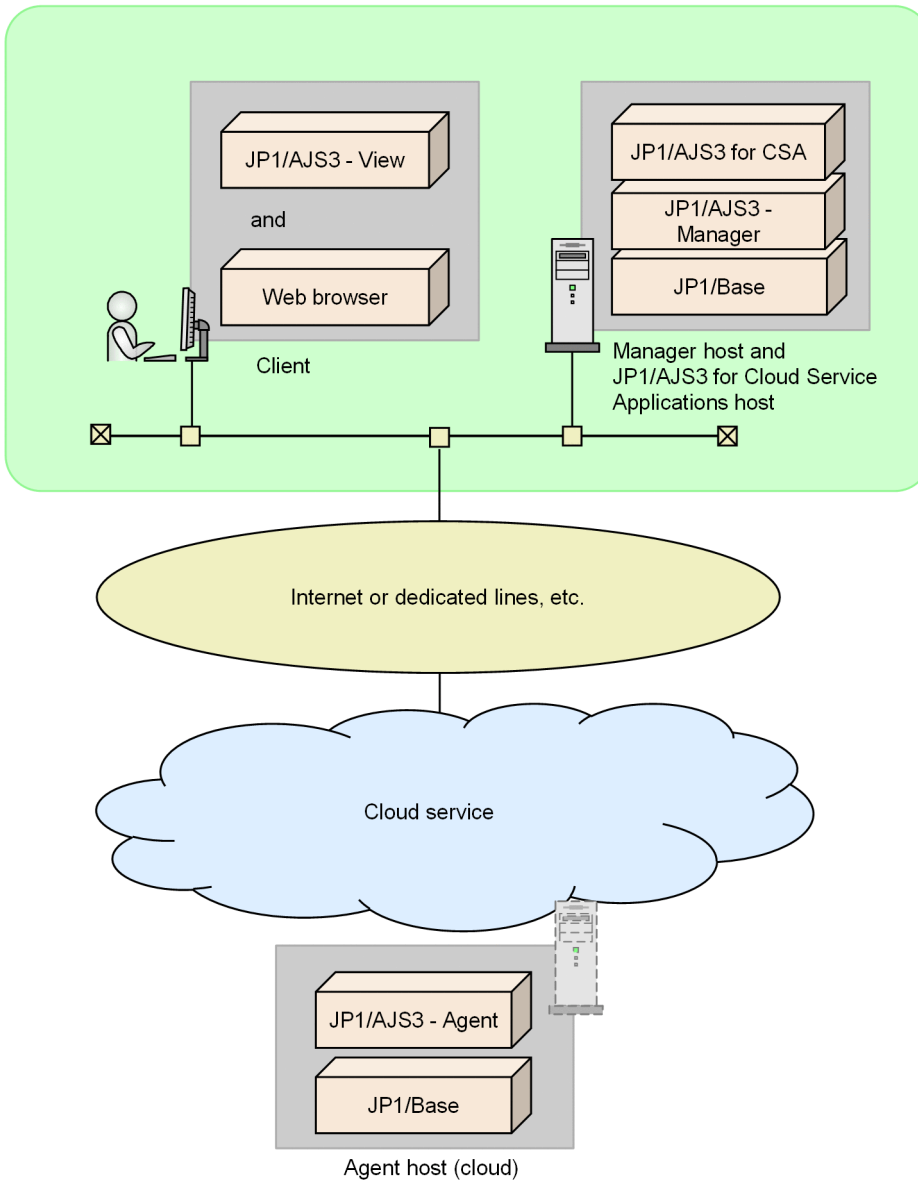
JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(4) To construct JP1/AJS3 - Manager and JP1/AJS3 - Agent in on-premises environment and on cloud in mix

JP1/AJS3 for Cloud Service Applications is constructed on an on-premises host while JP1/AJS3 - Manager and JP1/AJS3 - Agent are constructed in an on-premises environment and on a cloud in mix.

Figure 2–4: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - Manager in on-premises host and JP1/AJS3 - Agent in the cloud

On-premises



Legend:

JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

Notes

- JP1/AJS3 - Manager and JP1/AJS3 for Cloud Service Applications can also be constructed on another host.
- It is also possible to construct JP1/AJS3 - Manager on a cloud and JP1/AJS3 - Agent in an on-premises environment.

2.2.2 Use in cloud environment

This section explains the system configuration for constructing JP1/AJS3 for Cloud Service Applications in a cloud environment.

 **Note**

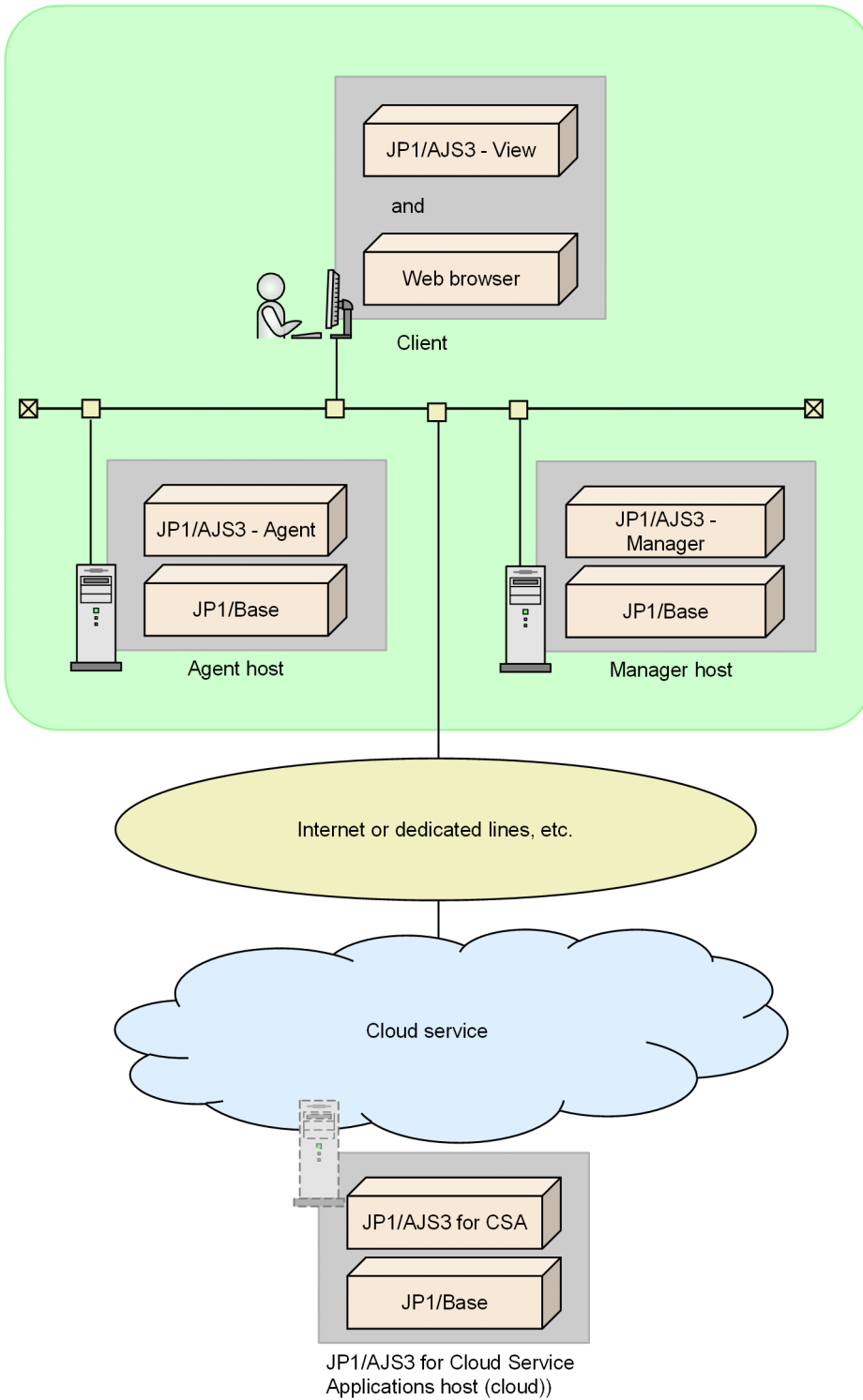
It is also possible to use the manager host as a service linkage job or service linkage monitoring job execution destination host without constructing an agent host.

(1) To construct JP1/AJS3 - Manager and JP1/AJS3 - Agent in on-premises environment

JP1/AJS3 for Cloud Service Applications is constructed on a cloud, and JP1/AJS3 - Manager and JP1/AJS3 - Agent are in an on-premises environment.

Figure 2–5: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications on cloud and JP1/AJS3 - Manager and JP1/AJS3 - Agent in the on-premises host

On-premises



Legend:

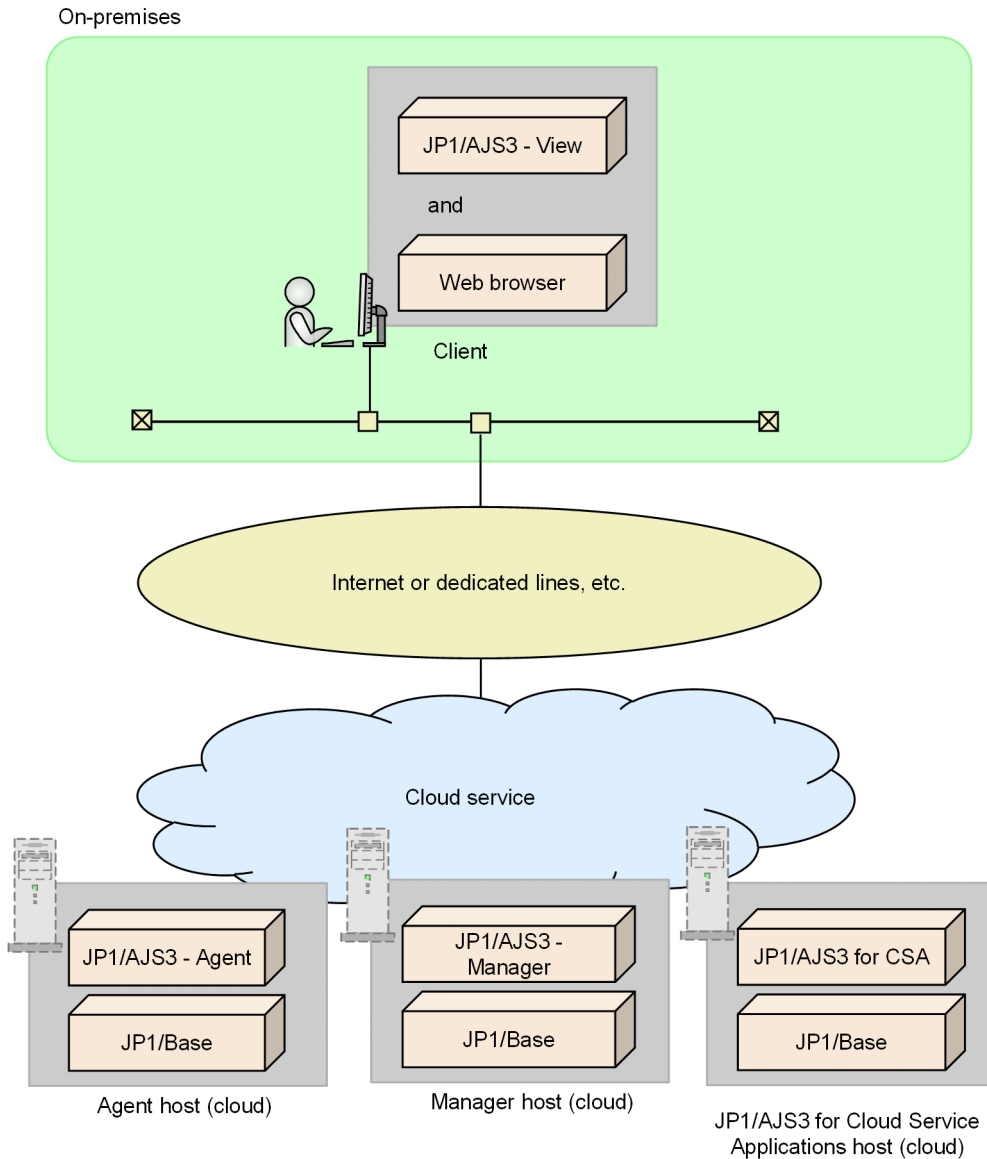
JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(2) To construct only JP1/AJS3 for Cloud Service Applications in cloud

JP1/AJS3 for Cloud Service Applications is constructed in a cloud host separate from the one for JP1/AJS3 - Manager and JP1/AJS3 - Agent.

JP1/AJS3 - Manager and JP1/AJS3 - Agent are also constructed in the cloud.

Figure 2–6: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager, and JP1/AJS3 - Agent in the cloud



Legend:

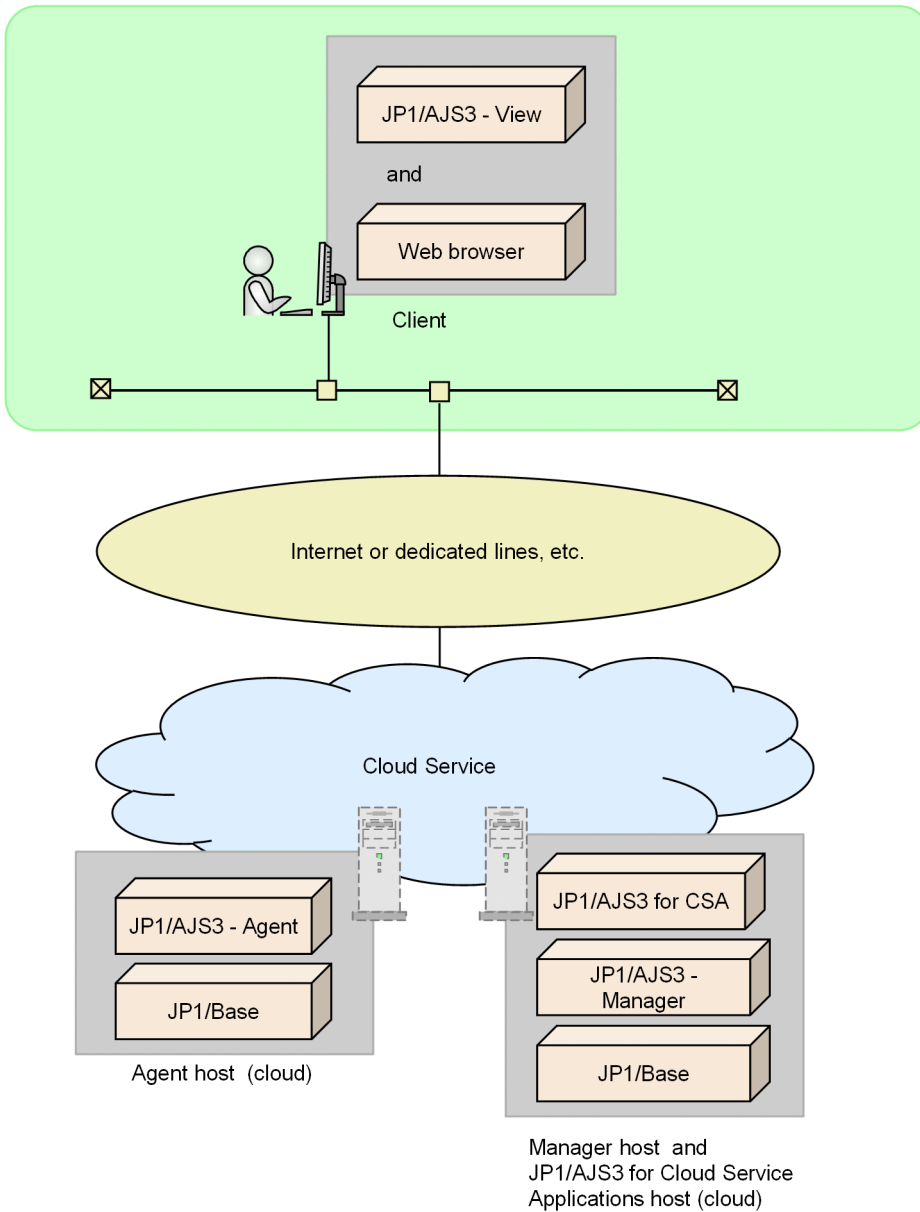
JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(3) To construct on the same host as JP1/AJS3 - Manager or JP1/AJS3 - Agent on cloud

JP1/AJS3 for Cloud Service Applications is constructed on the same host as the one for JP1/AJS3 - Manager or JP1/AJS3 - Agent in the cloud.

Figure 2–7: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications on the same cloud host for JP1/AJS3 - Manager

On-premises



Legend:

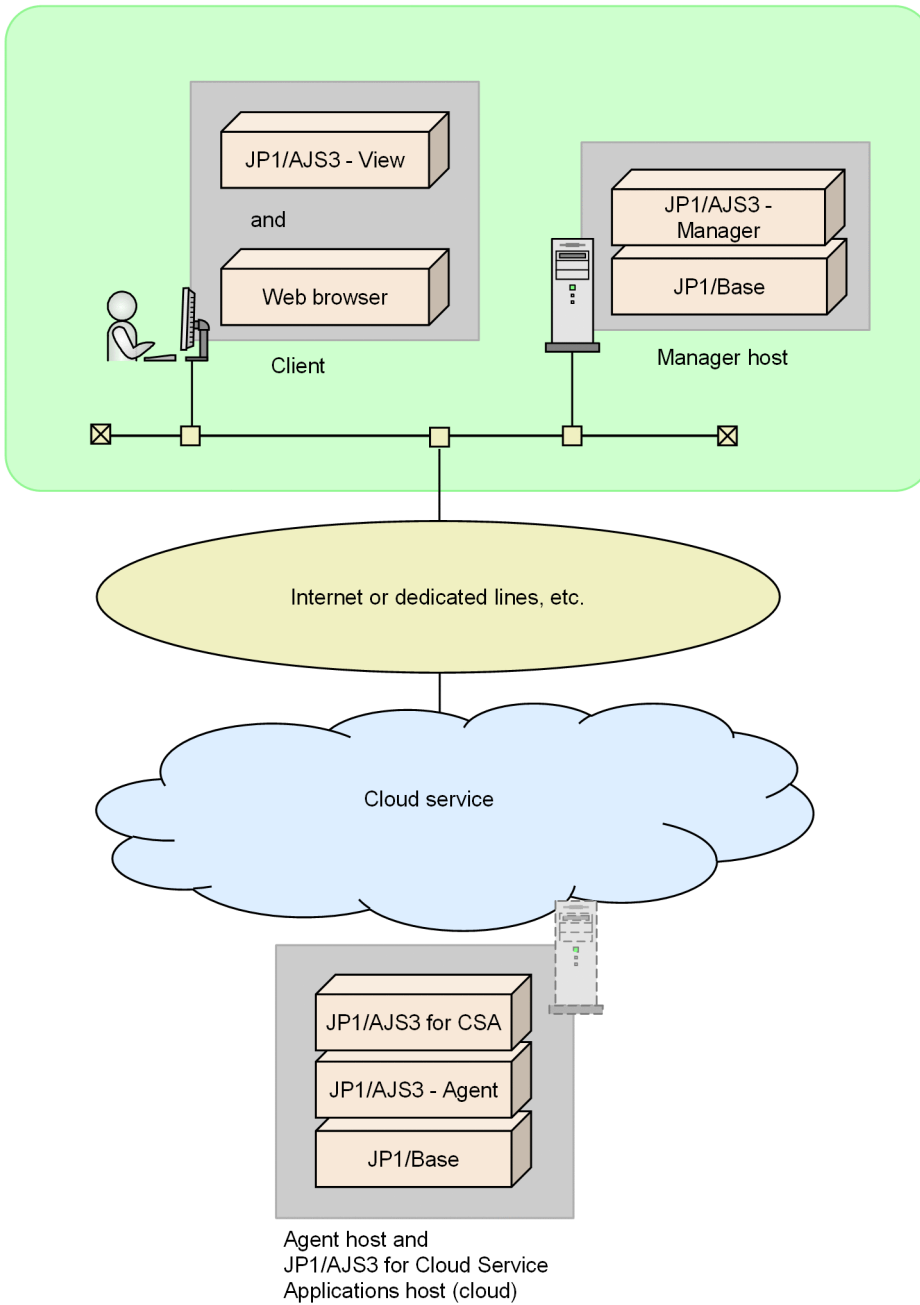
JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

(4) To construct JP1/AJS3 - Manager and JP1/AJS3 - Agent in a mix of on-premises and cloud

JP1/AJS3 for Cloud Service Applications is constructed on a host in a cloud, while JP1/AJS3 - Manager and JP1/AJS3 - Agent are constructed in a mixed environment of on-premises and cloud.

Figure 2–8: Example of system configuration for constructing JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - Agent in the cloud host and JP1/AJS3 - Manager in on-premises

On-premises



Legend:

JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

Notes

- JP1/AJS3 - Agent and JP1/AJS3 for Cloud Service Applications can be constructed on another host.
- It is possible to construct JP1/AJS3 - Manager in a cloud and JP1/AJS3 - Agent in an on-premises environment.

2.2.3 Configuration in cluster system

A cluster system operates multiple server systems in linkage as one system. By constructing two servers in the same environment and, if the server executing a business operation (execution system) fails, letting the server standing by (standby server) take over the processing, the business operation can be continued.

(1) Prerequisites of cluster system

When using JP1/AJS3 for Cloud Service Applications in a cluster system, the following prerequisites must be satisfied:

1. The cluster software must be a program that can control the following 2 to 4:
 2. It must be able to use a shared disk that can be taken over from the execution system to the standby system.
In particular, the following conditions must be satisfied:
 - The shared disk must be assigned before JP1/AJS3 for Cloud Service Applications is started.
 - The assignment of the shared disk must not be released while JP1/AJS3 for Cloud Service Applications is being executed.
 - The assignment of the shared disk must be released after JP1/AJS3 for Cloud Service Applications is stopped.
 - Exclusive control is carried out so that the shared disk can be accessed only from the execution system node.
 - Files must be protected by such a system as a file system with a journal function, so that the files will not be erased in case of a system failure.
 - Even in a case of failover, the contents written to files must be guaranteed and taken over.
 - Failover can be forcibly executed even if an ongoing process is using the shared disk.
 - Recovery processing that is performed if a failure in the shared disk is detected must be controlled by the cluster software and JP1/AJS3 for Cloud Service Applications does not have to be aware of the recovery processing. If starting or stopping JP1/AJS3 for Cloud Service Applications is necessary as an extension of the recovery processing, the cluster software must request JP1/AJS3 for Cloud Service Applications to execute starting or stopping.
 3. The IP address used for a cluster operation must satisfy the following conditions:
 - Communication must be able to be performed using an IP address that can be taken over and is used for a cluster operation.
 - The IP address used for a cluster operation must be uniquely determined from the host name used for a cluster operation.
 - The IP address used for a cluster operation must be assigned before JP1/AJS3 for Cloud Service Applications is started.
 - The IP address used for a cluster operation must not be deleted while JP1/AJS3 for Cloud Service Applications is being executed.
 - Correspondence between the host name used for a cluster operation and the IP address used for a cluster operation must not be changed while JP1/AJS3 for Cloud Service Applications is being executed.
 - The IP address used for a cluster operation must be deleted after JP1/AJS3 for Cloud Service Applications is stopped.
 - Recovery processing that is performed if a network failure in the shared disk is detected must be controlled by the cluster software, and JP1/AJS3 for Cloud Service Applications does not have to be aware of the recovery processing. If starting or stopping JP1/AJS3 for Cloud Service Applications is necessary as extension of the recovery processing, the cluster software must request JP1/AJS3 for Cloud Service Applications to execute starting or stopping.

- The host name used for a cluster operation must be set in the hosts file or name server and can be transmitted through TCP/IP communication.

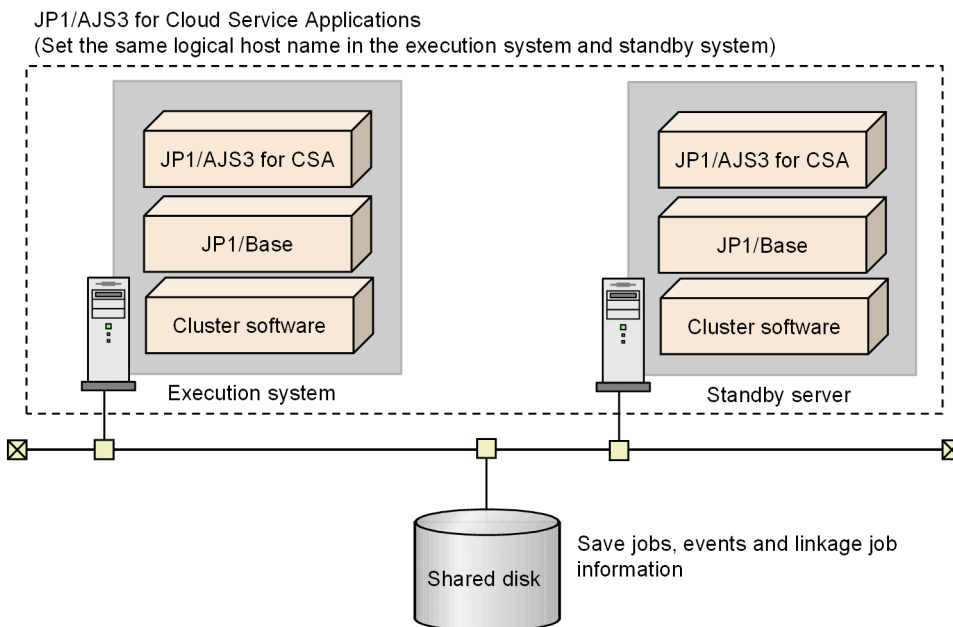
Unless the above conditions are satisfied, a problem may occur in the operation of JP1/AJS3 for Cloud Service Applications. For example, the following problems may occur:

- If data that was written by the execution system break at the time of failover, A problem of an error, data loss, or failure in starting may occur and JP1/AJS3 for Cloud Service Applications cannot operate correctly.
- If recovery processing is not performed even when an NIC failure occurs, A communication error occurs and JP1/AJS3 for Cloud Service Applications cannot operate correctly until NIC is changed through control by the cluster software or the server fails over to another server.

(2) System configuration to be supported

An example of system configuration for operating JP1/AJS3 for Cloud Service Applications in a cluster system is shown below.

Figure 2–9: Example of system configuration for operating JP1/AJS3 for Cloud Service Applications in a cluster system



Legend:

JP1/AJS3 for CSA: JP1/AJS3 for Cloud Service Applications

If a cloud service is supported, JP1/AJS3 for Cloud Service Applications created on a cloud can be configured in a cluster system.

! Important

- If a logical host environment is created for each of JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager, and JP1/AJS3 - Agent, they will fail over, in case of a failure, without affecting one another. It is therefore recommended to construct JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager, and JP1/AJS3 - Agent on different logical hosts.

- When considering system configuration during a cluster operation, a host name in FQDN format cannot be used as a logical host name.
- JP1/AJS3 for Cloud Service Applications can be set up with one logical host per physical host. This means that plural JP1/AJS3 for Cloud Service Applications of different logical host names cannot be set up on one physical host.
- JP1/AJS3 for Cloud Service Applications supports an active-standby cluster configuration. It does not support an active-active cluster configuration.
- When constructing JP1/AJS3 for Cloud Service Applications in a cluster configuration in a cloud environment, an IP address cannot be used as the host name of the JP1/AJS3 for Cloud Service Applications server.

For details on constructing JP1/AJS3 - Manager and JP1/AJS3 - Agent in a cluster system, refer to the description on the configuration example of a cluster system in the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*.

2.2.4 Operation in disaster-recovery configuration

Disaster recovery is a configuration to prepare for the contingencies of large-scale disasters by creating a system the same as the one that normally operates at a separate, remote location and copying the contents of the disk that has been updated during normal operation to the disk at the remote location.

To use JP1/AJS3 for Cloud Service Applications in a disaster-recovery configuration, the following operations must be performed as necessary:

- Backup and recovery of setup information and operation information
For details, refer to [3.7 Backup and recovery](#).
- Configurational change of the host name or IP address
For details, refer to [3.3.5 Changing the settings during operation](#).

For details when using JP1/AJS3 - Manager and JP1/AJS3 - Agent in the disaster-recovery configuration, refer to the description on the configuration example for disaster-recovery operation in the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*.

3

Designing and Building the System

This chapter describes the procedure for installing and setting up JP1/AJS3 for Cloud Service Applications.

The installation process requires administrator rights (for Windows) or superuser privileges (for Linux).

This chapter also describes backup and recovery procedures.

3.1 Installation

This section describes the procedure for installing JP1/AJS3 for Cloud Service Applications.

3.1.1 Installing JP1/Base

JP1/Base must be installed on the host where JP1/AJS3 for Cloud Service Applications will be installed. If JP1/Base is already installed on the host, it can be used.

After installing JP1/AJS3 for Cloud Service Applications, you must configure the user authentication feature and perform the following setup in JP1/Base before you can set up JP1/AJS3 for Cloud Service Applications. For details on Base versions that can be used, see [2.1.1 Prerequisite programs](#).

- Registering JP1 users who access the resources on JP1/AJS3 for Cloud Service Applications
Register the following JP1 users.
 - JP1 users who access JP1/AJS3 for Cloud Service Applications from clients.
 - JP1 users who execute service linkage jobs and service linkage monitoring jobs.
- Configuring access rights
Specify the permission level of a JP1 resource group for each registered JP1 user.

JP1/AJS3 for Cloud Service Applications provides access rights based on the following JP1 permission level names.

JP1_CSA_Admin

Administrator rights for JP1/AJS3 for Cloud Service Applications. This level has the rights to create, view, edit, and delete each definition of service linkage job information and service linkage monitoring job information.

JP1_CSA_AuthEditor

This level has the rights to create, view, edit, and delete authentication definitions.

JP1_CSA_Guest

This level has the rights to view each definition of service linkage job information and service linkage monitoring job information.

JP1_CSA_JobExec

This is the view permission when executing a service linkage job and a service linkage monitoring job. To execute a service linkage job and a service linkage monitoring job, a JP1 user requires this permission.

The JP1 users who log in to JP1/AJS3 for Cloud Service Applications to create, view, edit, and delete definitions of service linkage job information and service linkage monitoring job information must assign rights to the resource group JP1_CSA and the JP1 resource group in the definition.

For details of the installation and setup of JP1/Base, please see the *JP1/Base User's Guide*.

3.1.2 Installation (for Windows)

The following shows the procedure for an installation of JP1/AJS3 for Cloud Service Applications on a Windows host.

1. Log on as an administrator to the host where JP1/AJS3 for Cloud Service Applications will be installed.
2. Close all programs that will link with JP1/AJS3.

If you are using a program that will link with JP1/AJS3 on the host where JP1/AJS3 for Cloud Service Applications will be installed, please be sure to close it. If the Windows Event Viewer is open, please close it.

3. Set the media for JP1/AJS3 for Cloud Service Applications.

The Hitachi Integrated Installer screen appears.

4. Follow the instructions on screen to enter the necessary information and install the software.

The following shows the information to provide during installation.

- User information

Enter your user name and other information.

- Installation folder

Specify the folder where JP1/AJS3 for Cloud Service Applications will be installed. Do not install it in the same folder as another product.

5. The installation is complete. When a restart is requested, restart the host.

For the setup of JP1/AJS3 for Cloud Service Applications, please see [3.3 Setup](#).

Notes

- The installation folder specified when installing JP1/AJS3 for Cloud Service Applications must be 75 bytes or less in path length. Please make sure that the path to the installation folder does not contain multi-byte characters. The default installation folder for JP1/AJS3 for Cloud Service Applications is `C:\Program Files\Hitachi\JP1AJS3CSA`.
- JP1/AJS3 for Cloud Service Applications cannot be installed directly under a drive.
- If you are not the administrator when User Account Control (UAC) is enabled, you must be the administrator to install the software.
- For the folders and files that will be created during installation and notes, please see [A. Files and Directories](#).
- When you install JP1/AJS3 for Cloud Service Applications, the ports for internal communication (22267, 22268, and 22269) must be available. If you want to use them for other purposes, you must install JP1/AJS3 for Cloud Service Applications while they are available before you can change the ports to use.
- When you perform an upgrade installation, delete your web browser's cache. Otherwise, your web browser looks in the cache for the previous version and the information after the upgrade may not apply.

3.1.3 Installation (for Linux)

The following shows the procedure for an installation of JP1/AJS3 for Cloud Service Applications on a Linux host.

1. Log in as a superuser to the host where JP1/AJS3 for Cloud Service Applications will be installed, or switch to a superuser with the su command.

2. Close all programs that will link with JP1/AJS3 for Cloud Service Applications.

If you are using a program that will link with JP1/AJS3 for Cloud Service Applications on the host where JP1/AJS3 for Cloud Service Applications will be installed, please be sure to close it. If the Windows Event Viewer is open, please close it.

3. Set the media for JP1/AJS3 for Cloud Service Applications.

4. Mount the installation media.

Use `/mnt/dvdrom` as the mount directory. For the mount command, please see the OS documentation.

5. Execute the following command to start the Hitachi PP Installer.

```
/mnt/dvdrom/X64LIN/setup /mnt/dvdrom
```

6. Enter I on the initial screen.

A list of software that you can install is displayed.

7. Select the JP1/AJS3 series program that you want to install and enter I.

The selected program will be installed.

To select a program, move the cursor and use the space bar to select it.

8. After the installation is successfully completed, enter Q.

The initial screen of the Hitachi PP Installer appears again.

For the setup of JP1/AJS3 for Cloud Service Applications, please see [3.3 Setup](#).

Notes

- When you install JP1/AJS3 for Cloud Service Applications, the ports for internal communication (22267, 22268, and 22269) must be available. If you want to use them for other purposes, you must install JP1/AJS3 for Cloud Service Applications while they are available before you can change the ports to use.
- When you perform an upgrade installation, delete your web browser's cache. Otherwise, your web browser looks in the cache for the previous version and the information after the upgrade may not apply.

3.2 Uninstallation

This section describes the procedure for uninstalling JP1/AJS3 for Cloud Service Applications.

The uninstallation process requires administrator rights (for Windows) or superuser privileges (for Linux).

3.2.1 For Windows

This section describes the procedure for uninstalling JP1/AJS3 for Cloud Service Applications on a host that runs Windows.

1. Exit programs.

Close all programs before the uninstallation.

2. In Windows, from Control Panel - Add/Remove Programs, uninstall the program.

At Add/Remove Programs, select the program that you want to uninstall and uninstall it.

3. Delete user files.

When JP1/AJS3 for Cloud Service Applications is deleted, the files that were created by the user, such as definition files and log files created after installation, will not be deleted.

To delete these files, use Explorer to delete the folder where JP1/AJS3 for Cloud Service Applications was installed.

Note

If you are not the administrator when User Account Control (UAC) is enabled, you must be the administrator to uninstall the software.

3.2.2 For Linux

This section describes the procedure for uninstalling JP1/AJS3 for Cloud Service Applications on the host that runs Linux.

1. Exit programs.

Close all programs before the uninstallation.

2. Execute the following command to start the Hitachi PP Installer.

```
/etc/hitachi_setup  
or  
/etc/hitachi_x64setup
```

The Hitachi PP Installer is started and the initial screen appears.

3. Enter D on the initial screen.

A list of programs that you can uninstall is displayed.

4. Select the JP1/AJS3 series program that you want to uninstall and enter D.

The selected program will be uninstalled.

To select a program, move the cursor and use the space bar to select it.

5. After the uninstallation is successfully completed, enter Q.

The initial screen of the Hitachi PP Installer appears again.

6. Check the deleted files.

After deleting JP1/AJS3 for Cloud Service Applications, check if any of the following directories remain. If so, please delete them.

```
/opt/jp1ajs3csa  
/var/opt/jp1ajs3csa  
/etc/opt/jp1ajs3csa
```

3.3 Setup

This section describes the method for setting up JP1/AJS3 for Cloud Service Applications.

3.3.1 Setup for using service linkage jobs and service linkage monitoring jobs

This section describes the setup for using service linkage jobs and service linkage monitoring jobs at JP1/AJS3 for Cloud Service Applications.

(1) Setup flow

The following shows the flow for setting up JP1/AJS3 for Cloud Service Applications.

1. Set up the JP1/AJS3 for Cloud Service Applications server.
2. Set up the execution host for a service linkage job and a service linkage monitoring job.
3. Define the linkage job information.
4. Set up at JP1/AJS3 - View.

(2) Setting up the JP1/AJS3 for Cloud Service Applications server

The following shows the procedure for setting up the JP1/AJS3 for Cloud Service Applications server.

1. Configure JP1/Base's user authentication feature.
For details, please see [3.1.1 Installing JP1/Base](#).
2. Configure the JP1/AJS3 for Cloud Service Applications server as required.
For details, please see [3.3.1\(3\) Configuring the JP1/AJS3 for Cloud Service Applications server](#).
3. Configure the settings for SSL communication as required.
You can use SSL communication to allow the Web GUI and the JP1/AJS3 for Cloud Service Application server to communicate via HTTPS, preventing passwords and other information from being intercepted. Communication between the JP1/AJS3 for Cloud Service Application server and the execution host for a service linkage job and a service linkage monitoring job is also encrypted using SSL.
For the procedure for setting up SSL communication, please see [3.3.2 Setting up the SSL communication environment](#).
4. Configure the firewall settings.
When a firewall is used in the environment, please configure it so that communication between JP1/AJS3 for Cloud Service Applications and a Web browser can pass through the firewall.
For details about port number, please see [D. Port number to be set](#).
5. Start the services of JP1/AJS3 for Cloud Service Applications.
Start the following services.
 - JP1/AJS3 CSA Web Application Server service
 - JP1/AJS3 CSA HTTP Server service

6. Check that the following URL can be accessed with your Web browser.

Access the following URL and confirm that the Web GUI login screen appears.

`http://host-name-or-IP-address-of-the-CSA-server:port-number/ajscsa/login.html`

The default port number is 22265 for HTTP connection and 22266 for HTTPS connection.

To enable SSL communication and connect using HTTPS, start the URL with `https`.

(3) Configuring the JP1/AJS3 for Cloud Service Applications server

Configure the JP1/AJS3 for Cloud Service Applications server as required. Depending on your environment, edit the configuration files shown in the following table.

Table 3–1: Table 3-1 Configuration files for the JP1/AJS3 for Cloud Service Applications server environment

What you want to set or change	Settings file	Reference
Change the size and number of log files	Environment-settings file (<code>ajs3csaweb.conf</code>)	3.4.1
Change the default port number that receives connection requests from Web browsers	HTTP server definition file (<code>httpsd.conf</code>)	3.4.2
Enable SSL communication	HTTP server definition file (<code>httpsd.conf</code>)	3.3.2, 3.4.2
Change the default port number used for communication between the HTTP server and the J2EE server	HTTP server definition file (<code>httpsd.conf</code>)	3.4.2
	User property file for J2EE server (<code>usrconf.properties</code>)	3.4.3
Change the default port number for internal management of the J2EE server	User property file for J2EE server (<code>usrconf.properties</code>)	3.4.3
	System property file for server management commands (<code>usrconf.properties</code>)	3.4.5
Change the maximum size of the Java heap used by applications on the J2EE server	Option definition file for J2EE server (<code>usrconf.cfg</code>)	3.4.4

3.3.2 Setting up the SSL communication environment

To configure SSL communication at JP1/AJS3 for Cloud Service Applications, a server certificate is required on the server-side host and a root certificate is required on the client-side host. For the server and root certificates, please see the description of encryption of JP1/AJS3 communication by SSL in the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide*.

(1) Configuring JP1/AJS3 for Cloud Service Applications to communicate over SSL

The following shows the procedure for configuring the JP1/AJS3 for Cloud Service Applications to communicate with a client host over SSL.

1. Execute the command to create a private key.

Execute the following command. The command to use is different depending on the type of certificate to create. The following command creates a private key without a passphrase in PEM format. You cannot use a private key with a passphrase or one that is not in PEM format.

To create an RSA certificate

For Windows:

```
installation-folder-of-JP1/AJS3 for Cloud Service Applications\uCPSB\ht  
tpsd\sbin\openssl.bat genrsa -rand name-of-the-file-to-use-for-random-n  
umber-generation -out path-to-the-private-key-file bit-length-of-the-pr  
ivate-key
```

For Linux:

```
/opt/jplajs3csa/uCPSB/httpsd/sbin/openssl.sh genrsa -rand name-of-the-f  
ile-to-use-for-random-number-generation -out path-to-the-private-key-fi  
le bit-length-of-the-private-key
```

To create an ECDSA certificate

For Windows:

```
installation-folder-of-JP1/AJS3 for Cloud Service Applications\uCPSB\h  
ttpsd\sbin\openssl.bat ecpkcs8 -genkey -noout -rand name-of-the-file-t  
o-use-for-random-number-generation -name name-of-the-elliptic-curve -ou  
t path-to-the-private-key-file
```

For Linux:

```
/opt/jplajs3csa/uCPSB/httpsd/sbin/openssl.sh ecpkcs8 -genkey -noout -r  
and name-of-the-file-to-use-for-random-number-generation[:name-of-the-f  
ile-to-use-for-random-number-generation ...] -name name-of-the-elliptic  
-curve -out path-to-the-private-key-file
```

For the execute permissions of `openssl.bat` and `openssl.sh`, please see the official OpenSSL website.

Specify the following *path-to-the-private-key-file*.

For Windows

```
Installation-folder-of-JP1/AJS3 for Cloud  
Service Applications\uCPSB\httpsd\conf\ssl\server\httpsdkey.pem#
```

For Linux

```
/opt/jplajs3csa/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem#
```

For details of the command to create a private key, see the description of the command used to obtain a certificate for SSL communication in the *JP1/Automatic Job Management System 3 Configuration Guide*.

httpsdkey.pem is the name of the private key file. You can specify any name for the private key file.
If you want to change the private key file name from `httpsdkey.pem`, please also change the default encryption key file name `httpsdkey.pem` specified in the Web server definition file (`httpsd.conf`) that will be configured in a later step.

2. To create an ECDSA certificate, convert the format of the private key.

Execute the following command.

For Windows:

```
installation-folder-of-JP1/AJS3 for Cloud Service Applications\uCPSB\https  
d\sbin\openssl.bat pkcs8 -topk8 -in private-key-file-before-conversion -ou  
t private-key-file-after-conversion -nocrypt
```

For Linux:

```
/opt/jp1ajs3csa/uCPSB/httpsd/sbin/openssl.sh pkcs8 -topk8 -in private-key
-file-before-conversion -out private-key-file-after-conversion -nocrypt
```

For the execute permissions of `openssl.bat` and `openssl.sh`, please see the official OpenSSL website.

For details of the command to convert the format of a private key, see the description of the command used to obtain a certificate for SSL communication in the *JP1/Automatic Job Management System 3 Configuration Guide*.

3. Execute the command to create a certificate signing request (CSR).

Execute the following command.

For Windows:

```
installation-folder-of-JP1/AJS3 for Cloud Service Applications\uCPSB\https
d\sbin\openssl.bat req -new signature-algorithm -key path-to-the-private-k
ey-file -out path-to-the-CSR-file
```

For Linux:

```
/opt/jp1ajs3csa/uCPSB/httpsd/sbin/openssl.sh req -new signature-algorithm
-key path-to-the-private-key-file -out path-to-the-CSR-file
```

For the execute permissions of `openssl.bat` and `openssl.sh`, please see the official OpenSSL website.

For the *path-to-the-private-key-file*, specify the path specified for the command to create a private key in step 1. For the *path-to-the-CSR-file*, specify the output folder and CSR file name that you like.

For details of the command to create a certificate signing request (CSR), see the description of the command used to obtain a certificate for SSL communication in the *JP1/Automatic Job Management System 3 Configuration Guide*.

4. Send a CSR to the CA.

When you send a CSR to the CA, it issues a server certificate and a root certificate to validate the server certificate.

5. Obtain server and root certificates in PEM format from the CA.



Important

Server and root certificates cannot be used if they are not in PEM format.

You can specify any names for server and root certificate files.

In the Web server definition file (`httpsd.conf`), which will be configured in a later step, `httpsd.pem` is specified as the default server certificate. If you use this file name, you do not need to change the name of the server certificate file in the Web server definition file.

And the acquired root certificate is used when you configure how a service linkage job and a service linkage monitoring job communicate via SSL.

6. When you use an intermediate certificate, you must combine the server and intermediate certificates in one file.

Open both certificates in your text editor and paste the content of the intermediate certificate in the server certificate in the following order.

1. Server certificate
2. Intermediate certificate
3. Cross root certificate[#]

[#]: Only when you use a cross root certificate

7. Place the server certificate on the JP1/AJS3 for Cloud Service Applications server.

Place the server certificate in the following folder.

For Windows

Installation-folder-of-JP1/AJS3 for Cloud Service Applications\uCP SB\http sd\conf\ssl\server

For Linux

/opt/jp1ajs3csa/uCP SB/http sd/conf/ssl/server

8. Edit the Web server definition file (http sd.conf) to enable SSL communication.

Uncomment the SSL communication setting section of the Web server definition file (http sd.conf) to enable SSL communication.

The following shows a sample for Windows. In this sample, the port number for communication, the names of the server certificate and private key files, the version of TLS used for SSL communication, and the encryption types that can be used with TLS are left unchanged from the default settings (server certificate: http sd.pem, private key: http sdkey.pem, TLS version: TLSv1.2). Only the comment symbols (#) are deleted.

<Before>

```
:
Listen 22265
#Listen [::]:22265

#Listen 22266
#Listen [::]:22266
#<VirtualHost *:22266>
#  ServerName MyServer
#  SSLEngine On
#  SSLCertificateFile "C:/Program Files/HITACHI/JP1AJS3CSA/uCP SB/http sd/conf/ssl/server/http sd.pem"
#  SSLCertificateKeyFile "C:/Program Files/HITACHI/JP1AJS3CSA/uCP SB/http sd/conf/ssl/server/http sdkey.pem"
#  SSLProtocol +TLSv1.2
#  SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
#  SSLCipherSuite AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
#  AllowEncodedSlashes On
#</VirtualHost>
:
```

<After>

```
:
#Listen 22265
#Listen [::]:22265

Listen 22266
#Listen [::]:22266
<VirtualHost *:22266>
  ServerName MyServer
  SSLEngine On
  SSLCertificateFile "C:/Program Files/HITACHI/JP1AJS3CSA/uCP SB/http sd/conf/ssl/server/http sd.pem"
  SSLCertificateKeyFile "C:/Program Files/HITACHI/JP1AJS3CSA/uCP SB/http sd/conf/ssl/server/http sdkey.pem"
  SSLProtocol +TLSv1.2
  SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
  SSLCipherSuite AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
#</VirtualHost>
:
```

```
M-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
    AllowEncodedSlashes On
</VirtualHost>
:
```

If the port number for SSL communication, the names of the server certificate and private key files, the version of TLS used for SSL communication, and the encryption types that can be used with TLS are changed from the default values in your environment, please change these settings as required.

The following shows the default values in the Web server definition file (`httpsd.conf`).

- Port number for SSL communication: 22266
- Name of the server certificate file: `httpsd.pem`
- Name of the private key file: `httpsdkey.pem`
- Version of TLS used for SSL communication: TLSv1.2
- Encryption types that can be used with TLSv1.3:
 - `TLS_AES_128_GCM_SHA256`
 - `TLS_AES_256_GCM_SHA384`
- Encryption types that can be used with TLSv1.2:
 - `AES128-GCM-SHA256`
 - `AES256-GCM-SHA384`
 - `ECDHE-RSA-AES128-SHA256`
 - `ECDHE-RSA-AES256-SHA384`
 - `ECDHE-RSA-AES128-GCM-SHA256`
 - `ECDHE-RSA-AES256-GCM-SHA384`
 - `ECDHE-ECDSA-AES128-SHA256`
 - `ECDHE-ECDSA-AES256-SHA384`
 - `ECDHE-ECDSA-AES128-GCM-SHA256`
 - `ECDHE-ECDSA-AES256-GCM-SHA384`

For details of the Web server definition file (`httpsd.conf`), please see [3.4.2 Details on the settings in the HTTP server definition file \(httpsd.conf\)](#).

9. Edit the Web server definition file (`httpsd.conf`) to enable log output for SSL communication.

Uncomment the `LogFormat` and `CustomLog` sections of the Web server definition file (`httpsd.conf`) to enable log output for SSL communication. The following shows a sample for Windows.

<Before>

```
:
#LogFormat "%t %{version}c %{cipher}c %{clientcert}c" hws_ssl
#CustomLog "|\"C:/Program Files/HITACHI/JP1AJS3CSA/uCPSB/httpsd/sbin/rot
atelogs2.exe\" \"C:/Program Files/HITACHI/JP1AJS3CSA/uCPSB/httpsd/logs/ssl
\" 10240 8\"" hws_ssl
:
```

<After>

```
:
LogFormat "%t %{version}c %{cipher}c %{clientcert}c" hws_ssl
CustomLog "|\"C:/Program Files/HITACHI/JP1AJS3CSA/uCPSB/httpsd/sbin/rota
telogs2.exe\" \"C:/Program Files/HITACHI/JP1AJS3CSA/uCPSB/httpsd/logs/ssl\"
```



```
" 10240 8\" hws_ssl  
:
```

10. Restart the JP1/AJS3 CSA HTTP Server service.

11. Place the root certificate in PEM format on the destination execution host for a service linkage job and a service linkage monitoring job.

To verify the server certificate of the JP1/AJS3 for Cloud Service Applications server at the destination (execution host for a service linkage job and a service linkage monitoring job), place the root certificate of the CA that issued the server certificate of the JP1/AJS3 for Cloud Service Applications server at an arbitrary location on the destination host.

If a root certificate has already been placed on the destination host, please check whether the CA that issued the root certificate is the same as the CA from which the server certificate was obtained in step 3.

If the CA's are the same:

You can use the root certificate that is already placed as it is. You do not need to overwrite the root certificate.

If the CA's are different:

Please combine the root certificate that is already placed with the root certificate that you have obtained. In this case, please make sure that each root certificate corresponds to the relevant section of the combined root certificate so that you can replace the section appropriately when the root certificate expires. Because root certificates are encoded in Base64, you do not know which section corresponds to which root certificate when you check the combined file.

For details, please see the *JP1/Base User's Guide*.

(2) Configuring a service linkage job and a service linkage monitoring job to communicate via SSL.

The following shows the procedure for configuring a service linkage job and a service linkage monitoring job to communicate over SSL.

1. Check whether the root certificate of the destination JP1/AJS3 for Cloud Service Applications server is located on the execution host for a service linkage job and a service linkage monitoring job.

The root certificate for the JP1/AJS3 for Cloud Service Applications server is placed to configure JP1/AJS3 for Cloud Service Applications to communicate via SSL. For details, please see [3.3.2\(1\) Configuring JP1/AJS3 for Cloud Service Applications to communicate over SSL](#).

2. Enable SSL communication.

Enter the following information in the connection configuration file that describes the settings of a connection between a service linkage job and a service linkage monitoring job and the corresponding JP1/AJS3 for Cloud Service Applications server.

```
CAfile=full-path-name-of-the-file-placed-in-step-1
```

When you create a new connection configuration file, you must configure it. For details of a connection configuration file, please see [3.5.1 Connection configuration file](#).

(3) Configuring your Web browser to communicate over SSL.

The following shows the procedure for configuring your Web browser to communicate over SSL.

1. Allow SSL communication in your Web browser.

SSL/TLS must also be enabled in your Web browser. For the setting method, please see the documentation of your Web browser.

If SSL/TLS is disabled, the login screen will not appear even when you access the URL for SSL communication. If SSL/TLS is disabled after you log in, further operations will not be available.

3.3.3 Setting up the cluster environment

This section describes the installation and setup for cluster operation.

For an overview of cluster operation, please see the description of the cluster system in the *JP1/Automatic Job Management System 3 Administration Guide*.

(1) Notes for setting up a cluster system.

- Check whether the cluster software that you will use is supported before setup and operation. For details of setting up a cluster system, see the documentation of the cluster system that you will use.
- Please be sure to set up a cluster system in JP1/Base before setting up the system in JP1/AJS3 for Cloud Service Applications.
- Please install JP1/AJS3 for Cloud Service Applications on the primary and secondary nodes in the same drive and directory.
- To use SSL communication on a logical host in a cluster system, acquire a server certificate by using the host name of the logical host. Even if you acquire a server certificate by using the host name of the physical host, you cannot use it on the logical host. However, in the following case, you can use the same server certificate on the physical host as on the logical host.
 - If a logical host name is specified as the SAN on the server certificate of a physical host
 - If the server certificate of the physical host is a wildcard certificate and the specified host name matches the logical host name

For details on acquiring server certificates and configuring other SSL communication settings, see [3.3.2 Setting up the SSL communication environment](#).

(2) Installation for cluster operation

Install JP1/AJS3 for Cloud Service Applications on the local disks of the primary and secondary nodes. When installing it, specify the same drive and directory name for both the primary and secondary nodes.

Important

Do not install JP1/AJS3 for Cloud Service Applications on a shared disk.

(3) Setting up JP1/AJS3 for Cloud Service Applications

The following shows the method for setting up a cluster environment for JP1/AJS3 for Cloud Service Applications.

(a) Steps on the primary node

1. Set up JP1/AJS3 for Cloud Service Applications for cluster operation.
Execute the following command.

```
ajscsasetup -d shared-directory -h logical-host-name-of-JP1/Base -m
```

2. Register the JP1/AJS3 for Cloud Service Applications service in the cluster software that you will use.
For details, please see (4) *Registration to the cluster software*.

(b) Steps on the secondary node

1. Set up JP1/AJS3 for Cloud Service Applications for cluster operation.

Execute the following command.

```
ajscsasetup -d shared-directory -h logical-host-name-of-JP1/Base -s
```

2. Register the JP1/AJS3 for Cloud Service Applications service in the cluster software that you will use.
For details, please see (4) *Registration to the cluster software*.

(4) Registration to the cluster software

Register the JP1/AJS3 for Cloud Service Applications service in the cluster software that you will use.

For details of the registration method, please see the documentation of your cluster software. Please note the following in registration.

- Please make sure that the JP1/AJS3 for Cloud Service Applications service is inherited from the primary node to the second node along with the IP address and shared disk to be used.
- Please make sure that the IP address and shared disk are inherited and that JP1/Base is started on the secondary node before the JP1/AJS3 for Cloud Service Applications service is started.
- If the JP1/AJS3 for Cloud Service Applications service is configured to start automatically, please change the setting so that it does not start automatically.
- For other notes, please see *Notes for creating the system* in the *Release Notes*.

The following shows the information about JP1/AJS3 for Cloud Service Applications that is required for registering cluster software.

(a) For Windows

Services to configure in the cluster software.

Use the steps below to register services in the cluster software.

1. In Windows, go to **Control Panel** and **Administrative Tools** and select **Services**.
2. Change the **Startup Type** setting of the services to register in the cluster software from **Automatic** to **Manual**.

The following shows the services to register in the cluster software:

- JP1/AJS3 CSA HTTP Server service
- JP1/AJS3 CSA Web Application Server service

Change the **Startup Type** setting of these services from **Automatic** to **Manual**.

3. Register the JP1/AJS3 CSA Web Application Server service and the JP1/AJS3 CSA HTTP Server service in the cluster software so that they are started in this order.

The following shows the display and service names of the services to register in the cluster software.

JP1/AJS3 CSA HTTP Server service

- Display name: JP1/AJS3 CSA HTTP Server

- Service name: JP1_AJS3_CSA_HTTP_Server

JP1/AJS3 CSA Web Application Server service

- Display name: JP1/AJS3 CSA Web Application Server
- Service name: JP1_AJS3_CSA_Web_Application_Server

Starting/stopping services

You must use the cluster software to start or stop the services registered in the software.

Monitoring service operation

The cluster software monitors the start status of the services.

(b) For Linux

Table 3–2: Information about JP1/AJS3 for Cloud Service Applications that is required for registration in the cluster software.

Features to register	Description
Start	<p>Start JP1/AJS3 for Cloud Service Applications.</p> <p>Command to use</p> <pre>/etc/opt/jp1ajs3csa/jajs_csa</pre> <p>You must start it after the shared disk and logical IP address are available. For details of the <code>jajs_csa</code> command, please see <i>jajs_csa (Linux only)</i> in 7. <i>Commands</i>.</p>
Stop	<p>Stop JP1/AJS3 for Cloud Service Applications.</p> <p>Command to use</p> <pre>/etc/opt/jp1ajs3csa/jajs_csa_stop</pre> <p>You must stop it before the shared disk and logical IP address become unavailable. For details of the <code>jajs_csa_stop</code> command, please see <i>jajs_csa_stop (Linux only)</i> in 7. <i>Commands</i>.</p>
Monitor operations	<p>Check whether JP1/AJS3 for Cloud Service Applications has ended abnormally. The <code>ps</code> command is used to see if the process exists.</p> <p>Sample usage of the <code>ps</code> command</p> <pre>ps -ef grep "process-to-monitor" grep -v "grep"</pre> <p>The following shows the processes to monitor.</p> <ul style="list-style-type: none"> • JP1/AJS3 CSA HTTP Server service <code>/opt/jp1ajs3csa/uCPSB/httpsd/sbin/httpsd</code> • JP1/AJS3 CSA Web Application Server service <code>/opt/jp1ajs3csa/uCPSB/CC/server/bin/cjstartsv ajs3csa</code>
Forcibly terminate	Same as stop.

3.3.4 Setting up the execution host for service linkage jobs and service linkage monitoring jobs

This section describes the procedure for setting up the execution host for service linkage jobs and service linkage monitoring jobs.

(1) Configuring the connection with the JP1/AJS3 for Cloud Service Applications server

Configure the following settings to connect the execution host for service linkage jobs and service linkage monitoring jobs with the JP1/AJS3 for Cloud Service Applications server.

- Host name of the JP1/AJS3 for Cloud Service Applications server.
- Protocol for connecting with the JP1/AJS3 for Cloud Service Applications server.
- Port number for connecting with the JP1/AJS3 for Cloud Service Applications server.
- Connection timeout time with the JP1/AJS3 for Cloud Service Applications server.
- Settings for when a proxy is used to connect with the JP1/AJS3 for Cloud Service Applications server.
- Name of the certificate file required for SSL communication with the JP1/AJS3 for Cloud Service Applications server.
- Maximum time for processing during a single connection with the JP1/AJS3 for Cloud Service Applications server.
- Number of retries for a communication connection error with the JP1/AJS3 for Cloud Service Applications server.
- Retry interval for a communication connection error with the JP1/AJS3 for Cloud Service Applications server.

Configure these settings in the connection configuration file. For details of a connection configuration file, please see [3.5.1 Connection configuration file](#).

Configure these settings both on the physical host and on the logical host.

The following shows the procedure for configuring the connection configuration file.

1. Create a connection configuration file.

On the execution host for service linkage jobs and service linkage monitoring jobs, create a file in an arbitrary directory[#] and describe the settings.

The host name of the JP1/AJS3 for Cloud Service Applications server is required. Please be sure to specify it.

#

If the execution host for service linkage jobs and service linkage monitoring jobs has a cluster configuration, place the connection configuration file on a shared disk.

Configure the permissions of the connection configuration file so that service linkage jobs and service linkage monitoring jobs (OS user who executes the job) can reference it.

Important

If the connection configuration file contains security information, the user is responsible for managing it.

Note

Create a connection configuration file by copying the sample at the following location.

In Windows:

```
JP1/AJS3-installation-folder\conf\ajscsajob_network.conf.model
```

In Linux:

```
/etc/opt/jp1ajs2/conf/ajscsajob_network.conf.model
```

If the connection configuration file is stored in the following path, the operation of step 2 is not required.

In Windows (Physical host):

```
JP1/AJS3-installation-folder\conf\ajscsajob_network.conf
```

In Windows (Logical host):

```
shared-folder\jp1ajs2\conf\ajscsajob_network.conf
```

In Linux (Physical host):

```
/etc/opt/jp1ajs2/conf/ajscsajob_network.conf
```

In Linux (Logical host):

```
shared-directory/jp1ajs2/conf/ajscsajob_network.conf
```

- Execute the following command to set the path to the connection configuration file as an environment setting parameter of the execution host for service linkage jobs and service linkage monitoring jobs.

In Windows:

```
jajs_config -k [{JP1_DEFAULT|logical host}# \JP1AJS2\CSA\CSAJOBAGENT\AJSCSAEXEC "CSACONNECTCONFIG"="The full path of the connection configuration file that you placed in step 1"
```

In Linux:

```
jajs_config -k "[{JP1_DEFAULT|logical host}# \JP1AJS2\CSA\CSAJOBAGENT\AJSCSAEXEC" "CSACONNECTCONFIG"="The full path of the connection configuration file that you placed in step 1"
```

#

For {JP1_DEFAULT|*logical-host-name*}, specify JP1_DEFAULT for a physical host or *logical-host-name* for a logical host.

For details of environment setting parameters, see [E. JP1/AJS3 Environment Setting Parameters](#) and the description of environment setting parameters in the *JP1/Automatic Job Management System 3 Configuration Guide*.

(2) Configuring service linkage monitoring jobs

Configure environment setting parameters for executing service linkage monitoring jobs.

For details about environment setting parameters, see [6. Management operation of service linkage monitoring jobs](#) and [E. JP1/AJS3 Environment Setting Parameters](#) to configure required environment setting parameters, and then start the JP1/AJS3 service.

3.3.5 Changing the settings during operation

This section describes the setup procedures when you want to change settings during the operation of JP1/AJS3 for Cloud Service Applications.

(1) Changing the host name of the JP1/AJS3 for Cloud Service Applications server

The following shows the procedure for changing the host name of the JP1/AJS3 for Cloud Service Applications server.

Important

You must change the host name of the JP1/AJS3 for Cloud Service Applications server while service linkage jobs and service linkage monitoring jobs are not running.

1. Log out of all Web screens.
2. Stop the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service on the JP1/AJS3 for Cloud Service Applications server.
For Windows, stop the JP1/AJS3 CSA HTTP Server service and then stop the JP1/AJS3 CSA Web Application Server service.
For Linux, execute the following command.

```
jajs_csa_stop
```
3. Change the host name of the JP1/AJS3 for Cloud Service Applications server.
For how to change the host name, please see the OS manual.
4. If the communication encryption function is used and the host name is changed to a host name that is different from the CN or SAN in the server certificate, obtain the server certificate and place it again.
If the host name is changed to a host name that is different from the CN or SAN in the server certificate, please obtain the server certificate and place it again.
If the server certificate is obtained again and the issuing CA is different from the CA that issued the original server certificate, you must also obtain the root certificate and place it again.
5. Specify a new host name in the Web server definition file (httpsd.conf).
For details of the Web server definition file (httpsd.conf), please see [3.4.2 Details on the settings in the HTTP server definition file \(httpsd.conf\)](#).
6. Start the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service on the JP1/AJS3 for Cloud Service Applications server.
For Windows, stop the JP1/AJS3 CSA Web Application Server service and then stop the JP1/AJS3 CSA HTTP Server service.
For Linux, execute the following command.

```
jajs_csa
```
7. Change the host name of the JP1/AJS3 for Cloud Service Applications server in the connection configuration file so that the execution host for service linkage jobs and service linkage monitoring jobs can execute the job.

3.3.6 Setting automatic startup and termination of the JP1/AJS3 for Cloud Service Applications service

The JP1/AJS3 for Cloud Service Applications service can be started automatically when the system starts, and can be terminated automatically when the system terminates.

The following describes how to set automatic startup and termination of the JP1/AJS3 CSA HTTP Server service or the JP1/AJS3 CSA Web Application Server service.

(1) Setting automatic startup of the JP1/AJS3 CSA HTTP Server service or the JP1/AJS3 CSA Web Application Server service

To start the JP1/AJS3 CSA HTTP Server service or JP1/AJS3 CSA Web Application Server service automatically when the system starts, set the automatic start script. The following describes how to set the automatic start script:

1. Open the following file with a text editor such as vi:

```
/etc/rc.d/init.d/jp1ajs3csa
```

2. In the file, delete the shaded part shown below.

```
: # /etc/opt/jp1ajs3csa/jajs_csa
```

3. Close the file.

(2) Setting automatic termination of the JP1/AJS3 CSA HTTP Server service or the JP1/AJS3 CSA Web Application Server service

The following describes how to set the automatic termination script for the JP1/AJS3 CSA HTTP Server service or JP1/AJS3 CSA Web Application Server service:

1. Open the following file with a text editor such as vi:

```
/etc/rc.d/init.d/jp1ajs3csa
```

2. In the file, delete the shaded part shown below.

```
: # /etc/opt/jp1ajs3csa/jajs_csa_stop
```

3. Close the file.

(3) Setting the language type when the JP1/AJS3 CSA HTTP Server service and JP1/AJS3 CSA Web Application Server service are started

To set the language type when the JP1/AJS3 CSA HTTP Server service and JP1/AJS3 CSA Web Application Server service are started:

1. Open the following file with a text editor such as vi:

```
/etc/rc.d/init.d/jp1ajs3csa
```

2. In the file, change the shaded character shown below to any of the values indicated in the table:


```
LANG=C  
or  
LANG=en_US.UTF-8
```

Table 3–3: Value that can be set for LANG.

Language	Value that can be set for LANG
Japanese	<ul style="list-style-type: none">• ja_JP.UTF-8• ja_JP.utf8• ja_JP.SJIS^{#1}• ja_JP.sjis^{#1}
English	<ul style="list-style-type: none">• C• en_US.UTF-8^{#2}• en_US.utf8^{#2}

#1:

Can be used only in SUSE Linux.

#2:

Only 7-bit ASCII characters can be used. Do not use characters other than 7-bit ASCII characters.

3. Close the file.

3.4 Configuration file details (JP1/AJS3 for Cloud Service Applications)

This section describes the details of each configuration file of JP1/AJS3 for Cloud Service Applications.

3.4.1 Details of setting items of the environment setting file (ajs3csaweb.conf)

This subsection describes the details on the format of settings and the items to be set in the environment-settings file (`ajs3csaweb.conf`).

(1) File storage folder

The following describes the folders for storing the file `ajs3csaweb.conf` and the model file `ajs3csaweb.conf.model`.

(a) Model file storage folder

The following shows the folder storing the `ajs3csaweb.conf.model` file.

In Windows:

`JP1/AJS3-for-Cloud-Service-Applications-installation-folder\conf`

In Linux:

`/etc/opt/jp1ajs3csa/conf`

(b) ajs3csaweb.conf file storage folder

The following shows the folder storing the `ajs3csaweb.conf` file.

In Windows:

`JP1/AJS3-for-Cloud-Service Applications-installation-folder\conf#1`

`#:1`

In a cluster configuration, the file name is as follows:

`shared-folder\jp1ajs3csa\conf`

In Linux:

`/etc/opt/jp1ajs3csa/conf#2`

`#:2`

In a cluster configuration, the file name is as follows:

`shared-folder/jp1ajs3csa/conf`

(2) File-editing procedure

The following describes the procedure for editing the `ajs3csaweb.conf` file:

(a) In Windows

1. Stop the JP1/AJS3 CSA HTTP Server service and then stop the JP1/AJS3 CSA Web Application Server service. To make changes with respect to the logs for the `ajscsasetup` command, this operation is unnecessary.

2. Back up `ajs3csaweb.conf` to any folder.

To change the command log settings, you must change `ajs3csaweb.conf` in the installation folder instead of the one in the shared folder even in cluster operation. Please back up `ajs3csaweb.conf` in the installation folder.

3. To change the size or number of log files, delete the following files.

To change the settings for command logging

- All command logs
- The `ajscsasetup.mm` and `jajs_csa_service.mm` files under the `mmap` directory

To make changes with respect to the logs related to starting or stopping services (`jajs_csa_service`)

- All logs related to starting or stopping services.
- The `jajs_csa_service.mm` file under the `mmap` directory.

To change the settings for application server logging.

- All application server logs.
- The `appserver.mm` file under the `mmap` directory.

To change the settings for server job logging

- All server job logs.
- The `appserverjob.mm` file under the `mmap` directory.

4. Copy the model file `ajs3csaweb.conf.model` and rename it to `ajs3csaweb.conf`. In a cluster environment, you must conduct the following steps on `ajs3csaweb.conf` under the shared folder. However, to change the settings for command logging, please do so on the `ajs3csaweb.conf` in the installation folder.

5. Open the `ajs3csaweb.conf` file by using a text editor.

6. Modify the definitions to be changed.

7. Save the `ajs3csaweb.conf` file.

8. Start the JP1/AJS3 CSA Web Application Server service and then the JP1/AJS3 CSA HTTP Server service.

To make changes with respect to the logs for the `ajscsasetup` command, this operation is unnecessary.

(b) In Linux

1. Stop the JP1/AJS3 CSA HTTP Server and JP1/AJS3 CSA Web Application Server services by running the following command:

```
/etc/opt/jp1ajs3csa/jajs_csa_stop
```

To make changes with respect to the logs for the `ajscsasetup` command, this operation is unnecessary.

2. Back up `ajs3csaweb.conf` to any directory.

To change the command log settings, you must change `ajs3csaweb.conf` in the installation folder instead of the one in the shared folder even in cluster operation. Please back up `ajs3csaweb.conf` in the installation folder.

3. To change the size or number of log files, delete the following files.

To change the settings for command logging

- All `ajscsasetup` command logs.

- The `ajscssetup.mm` and `jajs_csa_service.mm` files under the `mmap` directory.

To make changes with respect to the logs for the commands for starting and stopping services (`jajs_csa` and `jajs_csa_stop`)

- All logs related to starting or stopping services.
- The `jajs_csa.mm` file and `jajs_csa_stop.mm` file under the `mmap` directory.

To change the settings for application server logging

- All application server logs.
- The `appserver.mm` file under the `mmap` directory.

To change the settings for server job logging

- All server job logs.
- The `appserverjob.mm` file under the `mmap` directory.

4. Copy the model file `ajs3csaweb.conf.model` and rename it to `ajs3csaweb.conf`. In a cluster environment, you must conduct the following steps on `ajs3csaweb.conf` under the shared folder. However, to change the settings for command logging, please do so also on the `ajs3csaweb.conf` in the installation folder.

5. Open the `ajs3csaweb.conf` file by using a text editor such as `vi`.

6. Modify the definitions to be changed.

7. Save the `ajs3csaweb.conf` file.

8. Start the JP1/AJS3 CSA HTTP Server and JP1/AJS3 CSA Web Application Server services by running the following command:

```
/etc/opt/jplajs3csa/jajs_csa
```

To make changes with respect to the logs for the `ajscssetup` command, this operation is unnecessary.

(3) When the setting takes effect

If you change it for the command log:

- When executing the `ajscssetup` command

If you change it, including other changes:

- When the JP1/AJS3 CSA Web Application Server service starts

(4) Format

The following shows the format of settings in the `ajs3csaweb.conf` file:

```
[ ]
HNTR_LOG_LEVEL=level-of-the-message-to-be-output-to-integrated-trace-log
HNTR_LOG_LANG=language-type-of-the-message-to-be-output-to-integrated-trace-log
SYS_LOG_LEVEL=level-of-the-message-to-be-output-to-Windows-event-log
SYS_LOG_LANG=language-type-of-the-message-to-be-output-to-Windows-event-log
COM_LOG_SIZE=size-of-a-command-log-file
COM_LOG_LEVEL=level-of-the-message-to-be-output-to-command-log
```

```

COM_LOG_NUM=number-of-command-log-files
COM_LOG_LANG=language-type-of-the-message-to-be-output-to-command-log
SERVER_LOG_APP_SIZE=size-of-an-application-server-log-file
SERVER_LOG_APP_LEVEL=level-of-the-message-to-be-output-to-application-server-log
SERVER_LOG_APP_NUM=number-of-application-server-log-files
SERVER_LOG_LANG=language-type-of-the-message-to-be-output-to-application-server-log
SERVER_LOG_JOB_SIZE=size-of-server-job-log-file
SERVER_LOG_JOB_LEVEL=level-of-the-message-to-be-output-to-server-job-log-file
SERVER_LOG_JOB_NUM=number-of-server-job-log-files
SERVER_LOG_APP_MON_SIZE=size-of-an-application-server-log-file-for-executing-service-linkage-monitoring-jobs
SERVER_LOG_APP_MON_LEVEL=level-of-the-message-to-be-output-to-application-server-log-for-executing-service-linkage-monitoring-jobs
SERVER_LOG_APP_MON_NUM=number-of-application-server-log-files-for-executing-service-linkage-monitoring-jobs
SERVER_LOG_JOB_MON_SIZE=size-of-a-server-job-log-file-for-executing-service-linkage-monitoring-jobs
SERVER_LOG_JOB_MON_LEVEL=level-of-the-message-to-be-output-to-server-job-log-for-executing-service-linkage-monitoring-jobs
SERVER_LOG_JOB_MON_NUM=number-of-server-job-log-files-for-executing-service-linkage-monitoring-jobs
USED_DEF_LIMIT=Retention period for service-linked job definitions used during job execution
SERVER_SESSION_TIMEOUT=HTTP-session-timeout-period

```

When writing a comment on a line, begin the comment line with a semi colon (;).

(5) Setting items

The following describes the items to be set. Delimit each item by using a linefeed.

(a) HNTR_LOG_LEVEL

The following describes the items to be set. Delimit each item by using a linefeed.

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(b) HNTR_LOG_LANG

Specify the language type of the messages to be output to the integrated trace log.

Specifiable values

system

Messages are output in the language type set in the OS.

In Windows, If the character encoding set in the OS is neither English ASCII encoding nor Shift-JIS encoding, English ASCII encoding is assumed to be specified.

In Linux, if the character code set in the OS is anything other than the English ASCII code and UTF-8 code, the English ASCII code is assumed.

C

Messages are output by using English ASCII encoding.

SJIS

In Windows, Messages are output by using Shift-JIS encoding. In Linux, unable to specify.

ja_JP.UTF-8 or ja_JP.utf8

In Linux, Messages are output by using UTF-8 encoding. In Windows, unable to specify.

en_US.UTF-8 or en_US.utf8

In Linux, Messages are output by using English ASCII encoding. In Windows, unable to specify.

Default value

system

Recommended value

Set the value appropriate for the operating environment.

(c) SYS_LOG_LEVEL

Specifies the message level to output to the Windows event log (for Windows) or syslog (Linux).

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(d) SYS_LOG_LANG

Specify the language type of the messages to be output to the Windows event log.

Important

In Linux, unable to specify.

Specifiable values

system

Messages are output in the language type set in the OS.

If the character encoding set in the OS is neither English ASCII encoding nor Shift-JIS encoding, English ASCII encoding is assumed to be specified.

C

Messages are output by using English ASCII encoding.

SJIS

Messages are output by using Shift-JIS encoding.

Default value

system

Recommended value

Set the value appropriate for the operating environment.

(e) COM_LOG_SIZE

Specify the size of a command log file.

Specifiable values

4 to 16, 384 (units: kilobytes)

Default value

128

Recommended value

Default value

(f) COM_LOG_LEVEL

Specify the level of the messages to be output to the command log.

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(g) COM_LOG_NUM

Specify the number of command log files.

Specifiable values

1 to 16 (units: files)

Default value

2

Recommended value

Default value

(h) COM_LOG_LANG

Specify the language type of the messages to be output to the command log.

Specifiable values

system

Messages are output in the language type set in the OS.

In Windows, If the character encoding set in the OS is neither English ASCII encoding nor Shift-JIS encoding, English ASCII encoding is assumed to be specified.

In Linux, if the character code set in the OS is anything other than the English ASCII code and UTF-8 code, the English ASCII code is assumed.

C

Messages are output by using English ASCII encoding.

SJIS

In Windows, Messages are output by using Shift-JIS encoding. In Linux, unable to specify.

ja_JP.UTF-8 or ja_JP.utf8

In Linux, Messages are output by using UTF-8 encoding. In Windows, unable to specify.

en_US.UTF-8 or en_US.utf8

In Linux, Messages are output by using English ASCII encoding. In Windows, unable to specify.

Default value

system

Recommended value

Set the value appropriate for the operating environment.

(i) SERVER_LOG_APP_SIZE

Specify the size of an application server log file.

Specifiable values

4 to 16,384 (units: kilobytes)

Default value

8,192

Recommended value

Default value

(j) SERVER_LOG_APP_LEVEL

Specify the level of the messages to be output to the application server log.

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(k) SERVER_LOG_APP_NUM

Specify the number of application server log files.

Specifiable values

1 to 16 (units: files)

Default value

2

Recommended value

Default value

(l) SERVER_LOG_LANG

Specify the language type of the messages to be output to the application server log.

Specifiable values

system

Messages are output in the language type set in the OS.

If the language type set in the OS is neither Japanese nor English, English is assumed to be specified.

ja

Messages are output in Japanese.

en

Messages are output in English.

Default value

system

Recommended value

Set the value appropriate for the operating environment.

(m) SERVER_LOG_JOB_SIZE

Specify the size of server job log file.

Specifiable values

4 to 16,384 (units: kilobytes)

Default value

11,264

Recommended value

Default value

Cautionary note

If you want to change the default values, you must check the output size of the server job log during job operation and verify the time period during which the log can be kept as history before you can change the values.

(n) SERVER_LOG_JOB_LEVEL

Specify the level of the messages to be output to the server job log file.

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(o) SERVER_LOG_JOB_NUM

Specify the number of server job log files.

Specifiable values

1 to 16 (units: files)

Default value

3

Recommended value

Default value

(p) SERVER_LOG_APP_MON_SIZE

Specify the size of the application server log file (for executing service linkage monitoring jobs).

Specifiable values

4 to 16,384 (units: kilobytes)

Default value

8,192

Recommended value

Default value

(q) SERVER_LOG_APP_MON_LEVEL

Specify the level of the messages to be output to the application server log (for executing service linkage monitoring jobs).

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(r) SERVER_LOG_APP_MON_NUM

Specify the number of application server job log files (for executing service linkage monitoring jobs).

Specifiable values

1 to 16 (units: files)

Default value

2

Recommended value

Default value

(s) SERVER_LOG_JOB_MON_SIZE

Specify the size of the server job log file (for executing service linkage monitoring jobs).

Specifiable values

4 to 16,384 (units: kilobytes)

Default value

11,264

Recommended value

Default value

Cautionary note

If you want to change the default values, you must check the output size of the server job log during job operation and verify the time period during which the log can be kept as history before you can change the values.

(t) SERVER_LOG_JOB_MON_LEVEL

Specify the level of the messages to be output to the server job log file (for executing service linkage monitoring jobs).

Specifiable values

none

No message is output.

error

Error messages are output.

warn

Error and warning messages are output.

info

Error, warning, and information messages are output.

Default value

info

Recommended value

Default value

(u) SERVER_LOG_JOB_MON_NUM

Specify the number of server job log files (for executing service linkage monitoring jobs).

Specifiable values

1 to 16 (units: files)

Default value

3

Recommended value

Default value

(v) USED_DEF_LIMIT

Specify the retention period for historical information on service linkage job definitions, service linkage monitoring job definitions, or authentication definitions that were used during job execution.

Specifiable values

0 to 366 (unit: days)

Default value

180

Recommended value

Set the value appropriate for the operating environment.

Cautionary note

If you set this value to 0, no history information is stored. Therefore, message KNBB2407-Q or KNBB2408-Q will not be displayed in the dialog when service linkage job definitions, service linkage monitoring job definitions, or authentication definitions that have a job execution history are updated or deleted on the Web screen. In addition, when you edit a service linkage job definition, service linkage monitoring job definition, or authentication definition, the message `The definition has a job execution history!` message will not be displayed.

(w) SERVER_SESSION_TIMEOUT

Specify the server session timeout time. If the specified amount of time has passed since the server receives a request for status acquisition, operation, etc. until the next request arrives, the HTTP session times out.

Specifiable values

900 to 3,600 (units: seconds)

Default value

900

Recommended value

Default value

(6) Examples

The following shows an example of definitions in the `ajs3csaweb.conf` file:

```
[ ]
HNTR_LOG_LEVEL=error
HNTR_LOG_LANG=system
SYS_LOG_LEVEL=error
SYS_LOG_LANG=system
COM_LOG_SIZE=10240
COM_LOG_LEVEL=info
COM_LOG_NUM=2
COM_LOG_LANG=system
SERVER_LOG_APP_SIZE=8192
SERVER_LOG_APP_LEVEL=info
SERVER_LOG_APP_NUM=2
SERVER_LOG_JOB_SIZE=8192
SERVER_LOG_JOB_LEVEL=info
SERVER_LOG_JOB_NUM=2
SERVER_LOG_APP_MON_SIZE=8192
SERVER_LOG_APP_MON_LEVEL=info
SERVER_LOG_APP_MON_NUM=2
SERVER_LOG_JOB_MON_SIZE=8192
SERVER_LOG_JOB_MON_LEVEL=info
SERVER_LOG_JOB_MON_NUM=2
SERVER_LOG_LANG=system
USED_DEF_LIMIT=180
SERVER_SESSION_TIMEOUT=900
```

(7) Notes

- Do not change the settings of items other than those explained herein.
- Do not insert a space before or after the equal sign in a definition line.
- Do not enter a linefeed in the middle of a definition line.
- If you specify a value for an item that cannot be set, the line including the item will be ignored.
- If an item to be set is not found, the default specification for that item is assumed for operation.
- If a setting is invalid, the JP1/AJS3 CSA Web Application Server service cannot start.
- The definition keys of setting items are not case sensitive, but set values are case sensitive.
- If the same setting item is defined on multiple lines, only the first line defining the setting item is valid.

3.4.2 Details on the settings in the HTTP server definition file (httpsd.conf)

This subsection describes the details on the format of settings and the items to be set in the HTTP server definition file (`httpsd.conf`).

(1) File storage folder

The following shows the folder storing the `httpsd.conf` file.

In Windows:

```
JP1/AJS3-for-Cloud-Service-Applicationse-installation-folder  
  \uCP SB\httpsd\conf
```

In Linux:

```
/opt/jp1ajs3csa/uCP SB/httpsd/conf
```

(2) File-editing procedure

The following describes the procedure for editing the `httpsd.conf` file. If you are operating in a cluster environment, follow the edit procedure to set the same definitions for the secondary node as those set for the primary node.

(a) In Windows:

1. Stop the JP1/AJS3 CSA HTTP Server service.
2. Back up the `httpsd.conf` file, and store the backup file in any folder.
3. Open the `httpsd.conf` file by using a text editor.
4. Modify the definitions to be changed.
5. Save the `httpsd.conf` file by using UTF-8 encoding.
6. Start the JP1/AJS3 CSA HTTP Server service.

(b) In Linux

1. Stop the JP1/AJS3 CSA HTTP Server service by running the following command:

```
/etc/opt/jplajs3csa/jajs_csa_stop -t http
```

2. Back up the `httpsd.conf` file, and store the backup file in any directory.
3. Open the `httpsd.conf` file by using a text editor such as `vi`.
4. Modify the definitions to be changed.
5. Save the `httpsd.conf` file.
6. Execute the following command to start JP1/AJS3 CSA HTTP Server service:

```
/etc/opt/jplajs3csa/jajs_csa -t http
```

(3) When the setting takes effect

When the JP1/AJS3 CSA HTTP Server service starts

(4) Format

The following shows the format of settings in the `httpsd.conf` file:

(Omitted)

```
ServerRoot "/opt/jplajs3csa/uCPSB/httpsd"
```

```
ServerName host-name-of-JP1/AJS3-for-Cloud-service-Applications
```

```
DocumentRoot "/opt/jplajs3csa/uCPSB/httpsd/htdocs"
```

(Omitted)

```
ProxyPass /ajscsa/ http://localhost:port-number-to-be-used-for-the-communication-between-HTTP-and-J2EE-servers/ajscsa/ timeout=3600 connectiontimeout=30 nocanon
```

```
ProxyPassReverse /ajscsa/ http://localhost:port-number-to-be-used-for-the-communication-between-HTTP-and-J2EE-servers/ajscsa/
```

(Omitted)

```
Listen port-number-for-the-reception-of-connection-requests-from-client
```

```
#Listen [::]:port-number-for-the-reception-of-connection-requests-from-client
```

```
#Listen port-number-for-the-reception-of-connection-requests-from-client-during-SSL-communication
```

```
#Listen [::]:port-number-for-the-reception-of-connection-requests-from-web-browser-during-SSL-communication
```

```
#<VirtualHost *:port-number-for-the-reception-of-connection-requests-from-client-during-SSL-communication>
```

```
# ServerName host-name-of-JP1/AJS3-for-Cloud-Service-Applications
```

```
# SSLEngine On
```

```
# SSLCertificateFile "JP1/AJS3-for-Cloud-Service-Applications-installation-folder/uCPSB/httpsd/conf/ssl/server/name-of-server-certification-file"
```

```
# SSLCertificateKeyFile "JP1/AJS3-for-Cloud-Service-Applications-installation-folder/uCPSB/httpsd/conf/ssl/server/name-of-private-key-file"
```

```
# AllowEncodedSlashes On
# SSLProtocol version-of-TLS-used-for-SSL-communication
# SSLCipherSuite TLSv1.3 list-of-cipher-types-available-with-TLSv1.3
# SSLCipherSuite list-of-cipher-types-available-with-TLSv1.2
#</VirtualHost>
```

Note that lines beginning with a hash mark (#) are comment lines.

(5) Setting items

The following describes the items to be set.

(a) Host name of JP1/AJS3 for Cloud Service Applications server

The host name of a JP1/AJS3 for Cloud Service Applications server is set automatically.

If you have changed the host name of the JP1/AJS3 for Cloud Service Applications server, change this setting manually.

(b) Port number to be used for communication between HTTP and J2EE servers.

Specify the port number of the port to be used for the communication between the HTTP and J2EE servers on the JP1/AJS3 for Cloud Service Applications server. The default is 22267.

When you want to change the port number from the default, change the port number so that it is appropriate to the environment. Make sure that the value set for the `ProxyPass` and `ProxyPassReverse` entries is the same as the value set for the `webserver.connector.nio_http.port` entry in the user properties file for J2EE server (`usrconf.properties`). For details, see [3.4.3 User property file for J2EE server \(`usrconf.properties`\)](#).

(c) Port number for the reception of connection requests from client

When not using SSL communication, specify the port number of the port at which the JP1/AJS3 for Cloud Service Applications server receives connection requests from the client. The default is 22265.

If you have changed the port number for the reception of connection requests from the web browser, change the port number setting.

(d) Port number for the reception of connection requests from client during SSL communication

When using SSL encryption for communication between the JP1/AJS3 for Cloud Service Applications server and a client, specify the port number of the port at which the JP1/AJS3 for Cloud Service Applications server receives connection requests from the client. The default is 22266.

To enable SSL communication, delete the hash mark (#) at the beginning of the definition line. If you have changed the port number for the reception of SSL communication from the web browser from the default setting, change the port number setting.

For details, see [3.3.2 Setting up the SSL communication environment](#).

(e) Name of server certification file

When using SSL encryption for communication between the JP1/AJS3 for Cloud Service Applications server and client, specify the name of the server certification file obtained from the CA. The default is `httpsd.pem`.

To enable SSL communication, delete the hash mark (#) at the beginning of the definition line, and then change the default setting to the name of the server certification file.

For details, see [3.3.2 Setting up the SSL communication environment](#).

(f) Name of private key file

When using SSL encryption for communication between the JP1/AJS3 for Cloud Service Applications server and client, specify the name of the private key file. The default is `httpsdkey.pem`.

To enable SSL communication, delete the hash mark (#) at the beginning of the definition line, and then change the default setting to the name of the private key file.

For details, see [3.3.2 Setting up the SSL communication environment](#).

(g) Version of TLS used for SSL communication.

Specify `+TLSv1.2` or `+TLSv1.3` as the version of the TLS protocol used for SSL communication. Only the specified version of the TLS protocol is enabled for SSL communication. You can also specify multiple versions in a space-separated list format.

Example:

In the following examples, Δ indicates a halfwidth space.

- To enable only TLSv1.2, specify the following:
`SSLProtocol Δ +TLSv1.2`
- To enable only TLSv1.3, specify the following:
`SSLProtocol Δ +TLSv1.3`
- To enable TLSv1.2 and TLSv1.3, specify the following:
`SSLProtocol Δ +TLSv1.2 Δ +TLSv1.3`

The default is `+TLSv1.2`.

To enable SSL communication, delete the hash mark (#) at the beginning of the definition line, and then edit the entry according to the TLS protocol versions to be used.

(h) List of cipher types available with TLSv1.3

Specify a list of cipher types available with TLSv1.3 in the following format:

```
SSLCipherSuite TLSv1.3 cipher-type-1:cipher-type-2:cipher-type-3...
```

You can specify the following values:

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`

By default, all specifiable values are specified.

To enable SSL communication, always delete the hash mark (#) at the beginning of the definition line even if you do not use TLSv1.3. If you use TLSv1.3, edit the entry according to the cipher types to be used.

(i) List of cipher types available with TLSv1.2

Specify a list of cipher types available with TLSv1.2 in the following format:

```
SSLCipherSuite cipher-type-1:cipher-type-2:cipher-type-3...
```

You can specify the following values:

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384

By default, all specifiable values are specified.

To enable SSL communication, always delete the hash mark (#) at the beginning of the definition line even if you do not use TLSv1.2. If you use TLSv1.2, edit the entry according to the cipher types to be used.

(6) Note

If a setting is invalid, the JP1/AJS3 CSA HTTP Server service cannot start.

3.4.3 User property file for J2EE server (usrconf.properties)

This subsection describes the details on the format of settings and the items to be set in the user properties file for J2EE server (usrconf.properties).

(1) File storage folder

The following shows the folder storing the `usrconf.properties` file.

In Windows:

```
JP1/AJS3-for-Cloud-Service Applications-installation-  
folder\uCPSB\CC\server\usrconf\ejb\ajs3csa
```

In Linux:

```
/opt/jp1ajs3csa/uCPSB/CC/server/usrconf/ejb/ajs3csa
```

(2) File-editing procedure

The following describes the procedure for editing the `usrconf.properties` file. If you are operating in a cluster environment, follow the edit procedure to set the same definitions for the secondary node as those set for the primary node.

(a) In Windows

1. Stop the JP1/AJS3 CSA HTTP Server service and then stop the JP1/AJS3 CSA Web Application Server service.
2. Back up the `usrconf.properties` file, and store the backup file in any folder.
3. Open the `usrconf.properties` file by using a text editor.
4. Modify the definitions to be changed.
5. Save the `usrconf.properties` file.
6. Start the JP1/AJS3 CSA Web Application Server service and then start the JP1/AJS3 CSA HTTP Server service.

(b) In Linux

1. Execute the following command to stop the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jplajs3csa/jajs_csa_stop
```

2. Back up the `usrconf.properties` file, and store the backup file in any directory.
3. Open the `usrconf.properties` file by using a text editor such as `vi`.
4. Modify the definitions to be changed.
5. Save the `usrconf.properties` file.
6. Execute the following command to start the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jplajs3csa/jajs_csa
```

(3) When the setting takes effect

When the JP1/AJS3 CSA Web Application Server service starts

(4) Format

The following shows the format of settings in the `usrconf.properties` file:

```
(omitted)
# Internal http server settings
ejbserver.http.port=port-number-for-the-internal-management-of-J2EE-server
(omitted)
# NIO HTTP Server settings
webserver.connector.ajp13.port=port-number-to-be-used-for-the-communication-
```

```
between-HTTP-and-J2EE-servers
#webserver.connector.ajp13.max_threads=10
(omitted)
#ejbserver.rmi.naming.port=port-number-for-the-internal-management-of-J2EE-s
erver
(omitted)
```

Note that lines beginning with a hash mark (#) are comment lines.

(5) Setting items

The following describes the items to be set.

(a) Port numbers for the internal management of a J2EE server

Specify the port numbers for the internal management of the J2EE server. The defaults are 22268 and 22269.

When you want to change a port number from its default, change the port number so that it is appropriate to the environment. Make sure that the setting value of `ejbserver.rmi.naming.port` matches the setting value of `ejbserver.rmi.naming.port` in the system properties file for server management commands (`usrconf.properties`). For details, see [3.4.5 System property file for server management commands \(`usrconf.properties`\)](#).

(b) Port number to be used for communication between HTTP and J2EE servers.

Specify the port number of the port to be used for the communication between the HTTP and J2EE servers on the JP1/AJS3 for Cloud Service Applications server. The default is 22267.

When you want to change the port number from the default, change the port number so that it is appropriate to the environment. Make sure that the setting value of `webserver.connector.nio_http.port` matches the setting value of `ProxyPass` and `ProxyPassReverse` in the web server definition file (`httpsd.conf`). For details, see [3.4.2 Details on the settings in the HTTP server definition file \(`httpsd.conf`\)](#).

(6) Notes

- Do not change the settings of items other than those explained herein.
- If a setting is invalid, the JP1/AJS3 CSA Web Application Server service cannot start.

3.4.4 Option definition file for J2EE server (`usrconf.cfg`)

This subsection describes the details on the format of settings and the items to be set in the option definition file for J2EE server (`usrconf.cfg`).

(1) File storage folder

The following shows the folder storing the `usrconf.cfg` file.

In Windows:

```
JP1/AJS3-for-Cloud-Service-Applications-installation-
folder\uCPSB\CC\server\usrconf\ejb\ajs3csa
```

In Linux:

```
/opt/jp1ajs3csa/uCPSB/CC/server/usrconf/ejb/ajs3csa
```

(2) File-editing procedure

The following describes the procedure for editing the `usrconf.cfg` file. If you are operating in a cluster environment, follow the edit procedure to set the same definitions for the secondary node as those set for the primary node.

(a) In Windows

1. Stop the JP1/AJS3 CSA HTTP Server service and then stop the JP1/AJS3 CSA Web Application Server service.
2. Back up the `usrconf.cfg` file, and store the backup file in any folder.
3. Open the `usrconf.cfg` file by using a text editor.
4. Modify the definitions to be changed.
5. Save the `usrconf.cfg` file.
6. Start the JP1/AJS3 CSA Web Application Server service and then start the JP1/AJS3 CSA HTTP Server service.

(b) In Linux

1. Execute the following command to stop the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jp1ajs3csa/jajs_csa_stop
```

2. Back up the `usrconf.cfg` file, and store the backup file in any directory.
3. Open the `usrconf.cfg` file by using a text editor such as `vi`.
4. Modify the definitions to be changed.
5. Save the `usrconf.cfg` file.
6. Execute the following command to start the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jp1ajs3csa/jajs_csa
```

(3) When the setting takes effect

When the JP1/AJS3 CSA Web Application Server service starts

(4) Format

The following shows the format of settings in the `usrconf.cfg` file:

```
(omitted)
# java vm options
#add.jvm.arg=-Xms256m
add.jvm.arg=-Xmx the maximum size of Java heap available to applications on
```

```
the JP1/AJS3 for Cloud Service Applications server
(omitted)
```

Note that lines beginning with a hash mark (#) are comment lines.

(5) Setting items

The following describes the items to be set.

(a) The maximum size of Java heap available to applications on the JP1/AJS3 for Cloud Service Applications server

Specify the maximum size of the Java heap available to applications on the JP1/AJS3 for Cloud Service Applications server.

Specifiable values

512 to 5120 (units: megabytes)

Default value

2048 (units: megabytes)

Recommended value

Default value

Always end the specified size value with the character "m".

If you change the maximum size from the default, specify a maximum size appropriate for system operation. For the memory requirements, see the *Release Notes*.

(6) Examples

The following shows an example of definitions in the `usrconf.cfg` file:

```
(omitted)
# java vm options
#add.jvm.arg=-Xms256m
add.jvm.arg=-Xmx2048m
(omitted)
```

(7) Notes

- Do not change the settings of items other than those explained herein.
- If a setting is invalid, the JP1/AJS3 CSA Web Application Server service cannot start.

3.4.5 System property file for server management commands (usrconf.properties)

This subsection describes the details on the format of settings and the items to be set in the system properties file for server management commands (`usrconf.properties`).

(1) File storage folder

The following shows the folder storing the `usrconf.properties` file.

In Windows:

```
JP1/AJS3-for-Cloud-Service-Applications-installation-folder\uCPSB\CC\admin\usrconf
```

In Linux:

```
/opt/jplajs3csa/uCPSB/CC/admin/usrconf
```

(2) File-editing procedure

The following describes the procedure for editing the `usrconf.properties` file. If you are operating in a cluster environment, follow the edit procedure to set the same definitions for the secondary node as those set for the primary node.

(a) In Windows

1. Stop the JP1/AJS3 CSA HTTP Server service and then stop the JP1/AJS3 CSA Web Application Server service.
2. Back up the `usrconf.properties` file, and store the backup file in any folder.
3. Open the `usrconf.properties` file by using a text editor.
4. Modify the definitions to be changed.
5. Save the `usrconf.properties` file.
6. Start the JP1/AJS3 CSA Web Application Server service and then start the JP1/AJS3 CSA HTTP Server service.

(b) In Linux

1. Execute the following command to stop the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jplajs3csa/jajs_csa_stop
```

2. Back up the `usrconf.properties` file, and store the backup file in any directory.
3. Open the `usrconf.properties` file by using a text editor such as `vi`.
4. Modify the definitions to be changed.
5. Save the `usrconf.properties` file.
6. Execute the following command to start the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service.

```
/etc/opt/jplajs3csa/jajs_csa
```

(3) When the setting takes effect

When the JP1/AJS3 CSA Web Application Server service starts

(4) Format

The following shows the format of settings in the `usrconf.properties` file:

```
(omitted)
ejbserver.rmi.naming.port=port-number-for-the-internal-management-of-J2EE-server
```

(5) Setting items

The following describes the items to be set.

(a) Port numbers for the internal management of a J2EE server

Specify the port numbers for the internal management of the J2EE server. By default, no setting items are specified. If no setting item is specified, the default 22269 is used.

When you want to change a port number from its default, change the port number so that it is appropriate to the environment. Make sure that the setting value of `ejbserver.rmi.naming.port` matches the setting value of `ejbserver.rmi.naming.port` in the user properties file for J2EE server (`usrconf.properties`). For details, see [3.4.3 User property file for J2EE server \(usrconf.properties\)](#).

(6) Notes

- Do not change the settings of items other than those explained herein.
- If a setting is invalid, the JP1/AJS3 CSA Web Application Server service cannot start.

3.5 Configuration file details (JP1/AJS3)

This section describes the details of each configuration file in JP1/AJS3.

3.5.1 Connection configuration file

This section describes the details of the description format and setting items of the connection configuration file.

Note

The connection configuration file must be located on the execution host for service linkage jobs and service linkage monitoring jobs.

(1) File storage folder

It is also optional for the file name and the folder or directory where you want to store the file. However, store it in a folder or directory where the absolute path containing the file name is no more than 255 bytes.

The following is the location of the sample file for the connection configuration file:

In Windows:

```
JP1/AJS3 - Manager or JP1/AJS3 - Agent installation folder\conf\ajscsajob_network.conf.model
```

In Linux:

```
/etc/opt/jplajs2/conf/ajscsajob_network.conf.model
```

(2) File-editing procedure

Copy the existing connection configuration file to any location for backup and edit it with your text editor. You can copy the sample connection configuration file from its storage location and edit it as required.

(3) When the setting takes effect

- When executing the next service linkage job.
- When a service linkage monitoring job is started next (including when monitoring is resumed after the service is restarted)

(4) Format

The following shows the format of connection configuration file:

```
CSAServerName=Host name of the JP1/AJS3 for Cloud Service Applications server  
CSAConnectProtocol=Protocol for a service linkages job to connect with the JP1/AJS3 for Cloud Service Applications server  
CSAConnectPortNumber=Port number for a service linkage job to connect with the JP1/AJS3 for Cloud Service Applications server
```

```
ConnectTimeout=Connection timeout time for connecting the JP1/AJS3 for Cloud Service Applications server
ProxyAddr=Proxy for communication with JP1/AJS3 for Cloud Service Applications server
CAFile=Name of the server certificate file to verify the server certificate for SSL communication with the JP1/AJS3 for Cloud Service Applications server
Timeout=Maximum time for processing during a single connection with the JP1/AJS3 for Cloud Service Applications server
CSAConnectRetryCount=Number of retries when the connection with the JP1/AJS3 for Cloud Service Applications server cannot be established
CSAConnectRetryInterval=Retry interval when the connection with the JP1/AJS3 for Cloud Service Applications server cannot be established
```

Note that lines beginning with a hash mark (#) are comment lines.

(5) Setting items

The following describes the items to be set.

(a) CSA ServerName

Specify the host name of the JP1/AJS3 for Cloud Service Applications server so that service linkage jobs and service linkage monitoring jobs connect to the JP1/AJS3 for Cloud Service Applications server.

This name must be able to be resolved from the execution host for service linkage jobs and service linkage monitoring jobs. For name resolution, `jp1hosts` information or `jp1hosts2` information is also effective. For details of `jp1hosts` or `jp1hosts2`, please see the *JP1/Base User's Guide*.

Important

This setting item cannot be specified with the IP address of the JP1/AJS3 for Cloud Service Applications server.

Specifiable number of characters

1 to 255 (units: bytes)

This setting item cannot be omitted. If it is omitted, the commands for a service linkage job terminate with a non-zero return code.

(b) CSAConnectProtocol

Specify the protocol for service linkage jobs and service linkage monitoring jobs to connect with the JP1/AJS3 for Cloud Service Applications server.

Specifiable values

- `http`
A non-SSL protocol is used to communicate with the JP1/AJS3 for Cloud Service Applications server.
- `https`
SSL is used to communicate with the JP1/AJS3 for Cloud Service Applications server.

Default value

`http`

If the `CSAConnectProtocol=` setting line is omitted, the default value is assumed to be set.

(c) **CSAConnectPortNumber**

Specify the port number for service linkage jobs and service linkage monitoring jobs to connect with the JP1/AJS3 for Cloud Service Applications server.

Specifiable values

0 to 65535 (units: port number)

Default value

22265

(d) **ConnectTimeout**

Specify the connection timeout time for connecting the JP1/AJS3 for Cloud Service Applications server with the destination host.

If communication with the destination host is not established after the time specified here has passed, the connection is retried as many times as the retry count specified in `CSAConnectRetryCount` and at the retry interval specified in `CSAConnectRetryInterval`.

Specifiable values

1 to 600 (units: seconds)

Default value

10 (units: seconds)

If the `ConnectTimeout=` setting line is omitted, the default value is assumed to be set.

Depending on the settings of the OS on which service linkage jobs and service linkage monitoring jobs run and the network settings of the system, a timeout may occur in a shorter time than the specified connection timeout time, resulting in a connection error.

For the settings of the OS, please see the OS manual.

(e) **ProxyAddr**

When you use a proxy for communication with JP1/AJS3 for Cloud Service Applications, specify the proxy to use.

If the `ProxyAddr=` setting line is omitted, no proxy is used (`http_proxy` environment variables, such as environment variables, are not enabled).

Allowable format

```
protocol://user:password@host-name-of-the-proxy-server:port-number
```

The *protocol* must begin with `http://` or `https://`. It is not case sensitive.

If the port number is omitted, 1080 is assumed.

Operation is not guaranteed if incorrect data is specified.



Important

For the *host-name-of-the-proxy-server*, specify a value that can be resolved from the execution host of the service linkage job and the service linkage monitoring job. You cannot resolve the name of the proxy server by using the `jp1hosts` or `jp1hosts2` information.

Allowable number of characters

- When it begins with `http://`, 8 to 2,083 bytes.
- When it begins with `https://`, 9 to 2,083 bytes.

(f) CAFile

If you want to verify the server certificate for SSL communication with the JP1/AJS3 for Cloud Service Applications server, specify the name of the server certificate file.

You can specify only a server certificate in PEM format. If you specify a server certificate in DER format, an error occurs.

If the `CAFile=` setting line is omitted, the server certificate is not verified.

Allowable number of characters

1 to 511 bytes (units: bytes)

(g) Timeout

Specify the maximum time for processing during a single connection with the JP1/AJS3 for Cloud Service Applications server.

If the process is not completed after the time specified here has passed, it is retried as many times as the retry count specified in `CSAConnectRetryCount` and at the retry interval specified in `CSAConnectRetryInterval`.

Specifiable values

1 to 86,400 (units: seconds)

Default value

600

If the `Timeout=` setting line is omitted, the default value is assumed to be set.

(h) CSAConnectRetryCount

Specify the number of retries when the connection with the JP1/AJS3 for Cloud Service Applications server cannot be established or when the processing time limit specified in `Timeout` is exceeded.

If the JP1/AJS3 for Cloud Service Applications server cannot be connected even after retrying as many times as the value specified here, or if the processing time limit is exceeded, the command for the service linkage job and the service linkage monitoring job will terminate with a non-zero return code.

Specifiable values

0 to 100 (units: number of retries)

If 0 is specified, no retry is conducted and the command for the service linkage job and the service linkage monitoring job terminates with a non-zero return code.

Default value

2

If the `CSAConnectRetryCount=` setting line is omitted, the default value is assumed to be set.

(i) CSAConnectRetryInterval

Specify the retry interval when the connection with the JP1/AJS3 for Cloud Service Applications server cannot be established or when the processing time limit specified in `Timeout` is exceeded and `CSAConnectRetryCount` is set to other than 0.

When `CSAConnectRetryCount=0`, this setting item is ignored.

Specifiable values

1 to 300 (units: seconds)

Default value

20

If the `CSAConnectRetryInterval=` setting line is omitted, the default value is assumed to be set.

(6) Notes

- A zero-byte line and a line containing only spaces are ignored.
- If there is a space or tab at the beginning or end of each line, the value after the space or tab is removed is considered the valid value.
- If the value contains spaces in the middle, they are considered part of the value. However, if the value contains a tab in the middle, the command for the service linkage job and the service linkage monitoring job terminates with a non-zero return code.

Example 1

When `CAFile=C:\AAAΔBBB\CAFileΔ`, the specified value is regarded as `CAFile=C:\AAAΔBBB\CAFile`.

(Legend) Δ: space

Example 2

When `CAFile=C:\AAA<\t>BBB\CAFileΔ`, an error occurs.

(Legend) <\t>: tab, Δ: space

- If the same setting item is defined on multiple lines, the last line is valid.
- If an unknown keyword exists, the service linkage job and the service linkage monitoring job terminates with a non-zero return code.
- Be sure to specify a value for each item. If no value is specified, the service linkage job and the service linkage monitoring job terminates with a non-zero return code.
- Each line must be within 4,096 bytes including a line feed code. If a specified line exceeds 4,096 bytes, the service linkage job and the service linkage monitoring job terminates with a non-zero return code.

3.6 JP1/AJS3 for Cloud Service Applications database file

This section describes the database files of JP1/AJS3 for Cloud Service Applications.

3.6.1 Details of database files

JP1/AJS3 for Cloud Service Applications uses the following database files.

(1) Database file storage location

In Windows, if the destination folder is under the default or system-protected folder:

`%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\database\AJSCSA.db`

The default value of `%ALLUSERSPROFILE%` is `system-drive\ProgramData`.

Folders protected by the system use the path to one of the following folders:

- Folder in `system-drive\Windows`
- Folder in `system-drive\Program Files`
- Folder in `system-drive\Program Files (x86)`

In Windows, if the destination folder is other than the above:

`JP1/AJS3-for-CSA-installation-folder\database\AJSCSA.db`

When using cluster operation on Windows:

`shared-folder\jp1ajs3csa\database\AJSCSA.db`

In Linux:

`/var/opt/jp1ajs3csa/database/AJSCSA.db`

When using cluster operation on Linux:

`shared-directory/jp1ajs3csa/database/AJSCSA.db`

(2) Tables in the database

Item number	Table name	Table contents
1	AJSCSADEFINITION	Definition table
2	AJSCSAEXECUTEHISTORY	Execution history table

(3) Database file permissions

In Windows:

"Full Control" in "Administrators"

(Inheritance is disabled, no other users and groups are allowed.)

In Linux:

Permissions: 600 (-rw-----)

Owner: root

Group: root

(4) Temporary file storage location

In Windows, if the installation folder is under the default or system-protected folder:

`%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\tmp`

The default value of `%ALLUSERSPROFILE%` is *system-drive*\ProgramData.

Folders protected by the system use the path to one of the following folders:

- Folder in *system-drive*\Windows
- Folder in *system-drive*\Program Files
- Folder in *system-drive*\Program Files (x86)

In Windows, if the installation folder is other than the above:

`JP1/AJS3-for-CSA-installation-folder\tmp`

In Linux:

`/var/opt/jp1ajs3csa/tmp`

(5) Maintaining database files

The database files used at JP1/AJS3 for Cloud Service Applications are automatically maintained each time they are registered, edited, or deleted on the Web screen of JP1/AJS3 for Cloud Service Applications.

Database files are maintained in the following order.

1. Maintain execution history tables.

The execution history tables are maintained (records that have exceeded their retention period are deleted) when database files are automatically backed up.

2. Release invalid space in the entire database files.

3. Back up the entire database files.

While the database files are maintained, the following message log is output to the application server log.

If maintenance is successful

- KNBB3801-I
- KNBB3803-I
- KNBB3805-I

If an error occurs during maintenance

- KNBB3802-W
- KNBB3804-W
- KNBB3806-W



Note

Even if maintenance fails, the Web screen does not indicate it. The failure record is kept only in the application server log.

If an error occurs while the execution history tables are maintained or invalid space in the entire database files is released, no further maintenance is conducted.

(6) Backing up database files automatically

The database files used by JP1/AJS3 for Cloud Service Applications are backed up automatically. The storage location for database file backups is shown below.

In Windows, if the installation folder is under the default or system-protected folder:

`%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\database\AJSCSA.db.back`

The default value of `%ALLUSERSPROFILE%` is *system-drive*\ProgramData.

Folders protected by the system use the path to one of the following folders:

- Folder in *system-drive*\Windows
- Folder in *system-drive*\Program Files
- Folder in *system-drive*\Program Files (x86)

In Windows, if the installation folder is other than the above:

`JP1/AJS3-for-CSA-installation-folder\database\AJSCSA.db.back`

When using cluster operation on Windows:

`shared-folder\jp1ajs3csa\database\AJSCSA.db.back`

In Linux:

`/var/opt/jp1ajs3csa/database/AJSCSA.db.back`

When using cluster operation on Linux:

`shared-directory/jp1ajs3csa/database/AJSCSA.db.back`

3.7 Backup and recovery

This section describes the backup and recovery of the configuration information for JP1/AJS3 for Cloud Service Applications.

Back up the configuration information for JP1/AJS3 for Cloud Service Applications in case a failure occurs and the system breaks down. Make a backup when the system is changed, such as when JP1/AJS3 for Cloud Service Applications is set up.

3.7.1 the configuration information for JP1/AJS3 for Cloud Service Applications Backing up

This section describes the tasks required when backing up the configuration information for JP1/AJS3 for Cloud Service Applications.

For the files and directories related to JP1/AJS3 for Cloud Service Applications, please see *A. Files and Directories*.

(1) Backing up the configuration information for JP1/Base

Back up the configuration information for JP1/Base. For details, please see the *JP1/Base User's Guide*.

(2) Backing up the configuration information for the JP1/AJS3 for Cloud Service Applications server

Back up the files of JP1/AJS3 for Cloud Service Applications shown in the following table.

Table 3–4: Files to back up (in a normal configuration)

File name (In Windows)	File name (In Linux)	Contents
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \conf\ajs3csaweb.conf	/etc/opt/jplajs3csa/conf/ajs3csaweb.conf	Environment-settings file
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCPSB\httpsd\conf\ssl\server\httpsdkey.pem	/opt/jplajs3csa/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem	Server private key
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCPSB\httpsd\conf\ssl\server\newcert.pem	/opt/jplajs3csa/uCPSB/httpsd/conf/ssl/server/newcert.pem	SSL server certificate
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCPSB\httpsd\conf\httpsd.conf	/opt/jplajs3csa/uCPSB/httpsd/conf/httpsd.conf	Web server definition file
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCPSB\CC\server\usrconf\ejb\ajs3csa\usrconf.properties	/opt/jplajs3csa/uCPSB/CC/server/usrconf/ejb/ajs3csa/usrconf.properties	User property file for J2EE server

File name (In Windows)	File name (In Linux)	Contents
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\CC\server\usrconf\ejb\ajs3csa\usrconf.cfg	/opt/jplajs3csa/uCP SB/CC/server/usrconf/ejb/ajs3csa/usrconf.cfg	Option definition file for the J2EE server
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\CC\admin\usrconf\usrconf.properties	/opt/jplajs3csa/uCP SB/CC/admin/usrconf/usrconf.properties	System properties file for the server management command
%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\database\AJSCSA.db %ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\database\AJSCSA.db.back	/var/opt/jplajs3csa/database/AJSCSA.db /var/opt/jplajs3csa/database/AJSCSA.db.back	Database file

Table 3–5: Files to back up (in a cluster configuration)

File name (In Windows)	File name (In Linux)	Contents
<i>shared-folder</i> \jplajs3csa\conf\ajs3csaweb.conf	<i>shared-directory</i> /jplajs3csa/conf/ajs3csaweb.conf	Environment-settings file
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\httpsd\conf\ssl\server\httpsdkey.pem	/opt/jplajs3csa/uCP SB/httpsd/conf/ssl/server/httpsdkey.pem	Server private key
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\httpsd\conf\ssl\server\newcert.pem	/opt/jplajs3csa/uCP SB/httpsd/conf/ssl/server/newcert.pem	SSL server certificate
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\httpsd\conf\httpsd.conf	/opt/jplajs3csa/uCP SB/httpsd/conf/httpsd.conf	Web server definition file
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\CC\server\usrconf\ejb\ajs3csa\usrconf.properties	/opt/jplajs3csa/uCP SB/CC/server/usrconf/ejb/ajs3csa/usrconf.properties	User property file for J2EE server
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\CC\server\usrconf\ejb\ajs3csa\usrconf.cfg	/opt/jplajs3csa/uCP SB/CC/server/usrconf/ejb/ajs3csa/usrconf.cfg	Option definition file for the J2EE server
<i>JP1/AJS3-for-Cloud-Service-Applications-installation-folder</i> \uCP SB\CC\admin\usrconf\usrconf.properties	/opt/jplajs3csa/uCP SB/CC/admin/usrconf/usrconf.properties	System properties file for the server management command
<i>shared-folder</i> \jplajs3csa\database\AJSCSA.db <i>shared-folder</i> \jplajs3csa\database\AJSCSA.db.back	<i>shared-directory</i> /jplajs3csa/database/AJSCSA.db <i>shared-directory</i> /jplajs3csa/database/AJSCSA.db.back	Database file

3.7.2 the configuration information for JP1/AJS3 for Cloud Service Applications Recovering

This section describes the tasks required when recovering the configuration information for JP1/AJS3 for Cloud Service Applications.

(1) Recovering JP1/Base

After JP1/Base is set up, recover the physical and logical host environments. For the settings required for recovery, please see the *JP1/Base User's Guide*.

(2) Recovering the JP1/AJS3 for Cloud Service Applications server

Recover the JP1/AJS3 for Cloud Service Applications server using the following procedure.

1. Rebuild the JP1/AJS3 for Cloud Service Applications server (install the software and set up a cluster in the case of a cluster environment).
2. Place the backed-up configuration information file of the JP1/AJS3 for Cloud Service Applications server at its original location.
If you want to recover the backed-up database while the JP1/AJS3 for Cloud Service Applications service is running, please rename `AJSCSA.db.back` to `AJSCSA.db` and place it at its original location.
3. Start the JP1/AJS3 CSA Web Application Server service.
4. Start the JP1/AJS3 CSA HTTP Server service.

3.7.3 Backing up and recovering the entire system

You can back up and recover the entire system of JP1/AJS3 for Cloud Service Applications by using OS commands and backup tools. When you back up and recover the entire system, please note the following.

- Stop the JP1/AJS3 for Cloud Service Applications service.
- For cluster operation, please back up and recover both the local disk and the shared disk.
- If a service linkage job or service linkage monitoring job is executed while the service is stopped, the job will end abnormally. Please execute this procedure when no service linkage job or service linkage monitoring job is executed.

3.8 Notes when running anti-virus software

If anti-virus software imposes an exclusive control lock on a file or folder used by JP1/AJS3 for Cloud Service Applications, the following problems might arise:

- JP1/AJS3 for Cloud Service Applications does not start.
An exclusive control lock placed on a definition file that JP1/AJS3 for Cloud Service Applications references at startup might prevent JP1/AJS3 for Cloud Service Applications from starting.
- Service linkage jobs and service linkage monitoring jobs fail to execute or are delayed.
An exclusive control lock placed on a file needed to execute a service linkage job or service linkage monitoring job might prevent the job from starting, cause it to terminate abnormally, or delay its execution.
- You cannot change definitions.
An exclusive control lock placed on a JP1/AJS3 for Cloud Service Applications definition file might prevent you from adding or changing a job definition.
- JP1/AJS3 cannot output log data.
An exclusive control lock placed on a JP1/AJS3 for Cloud Service Applications definition file might prevent you from adding or changing a job definition.
- JP1/AJS3 for Cloud Service Applications commands end abnormally.
An exclusive control lock placed on a file used by a JP1/AJS3 for Cloud Service Applications command might cause the command to end abnormally.

If you run a virus check during JP1/AJS3 for Cloud Service Applications operation, exclude the following files and folders. If you run a virus check while JP1/AJS3 for Cloud Service Applications is stopped, make sure that the anti-virus program has finished checking the following files and folders before you restart JP1/AJS3 for Cloud Service Applications.

For details about the notes on JP1/AJS3, see the notes on running antivirus software in the manual *JP1/Automatic Job Management System 3 Design Guide (System Construction)*.

In Windows:

- Common files and folders of JP1/AJS3 for Cloud Service Applications that belong to the following categories:
 - JP1/AJS3 for Cloud Service Applications log files and folders
 - Files and folders that users can reference
 - Files and folders that users have no need to reference or modifyFor information about these files and folders, see *A. Files and Directories*.
- In `system-drive\Program Files\Hitachi\HNTRLib2`

In Linux:

- Files and folders of JP1/AJS3 for Cloud Service Applications that belong to the following categories:
 - JP1/AJS3 for Cloud Service Applications log files and folders
 - Files and folders that users can reference
 - Files and folders that users have no need to reference or modifyFor information about these files and folders, see *A. Files and Directories*.
- In `/opt/hitachi/HNTRLib2/`
- In `/var/opt/hitachi/HNTRLib2/`

If you run the data collection tool while a virus check is in progress, exclude the following files and folders, in addition to those listed above, from the virus check.

- Files collected for troubleshooting purposes.
 - Operating system log information required to troubleshoot JP1/AJS3 for Cloud Service Applications problems.
 - JP1-related information required to troubleshoot JP1/AJS3 for Cloud Service Applications problems.

For information about these files, see [9.2 Types of log information and storage locations](#).

- Destination folder for data acquired by the data collection tool.

4

Designs and definitions of linkage jobs

This chapter describes the procedures for defining the following linkage jobs using JP1/AJS3 for Cloud Service Applications:

- Service linkage job
- Service linkage monitoring job

4.1 Designs of linkage jobs

This section describes the design of linkage jobs.

4.1.1 Flow of designing linkage jobs

(1) Design of service linkage jobs

The service linkage jobs of JP1/AJS3 for Cloud Service Applications define how to link the cloud services to be linked. The flow for designing a service linkage job is as follows.

1. Consider the flow of jobs linked to cloud services, and then decide on the cloud services to execute as JP1/AJS3 jobs or jobnets.
2. Investigate and consider the specifications of the relevant cloud services and the command interfaces that can be linked.
3. Design the processing for connecting to the cloud service.
4. Design the method for managing information for performing authentication with the cloud service.
5. Design the processing for linking to the cloud service.

Based on the content designed in 3, 4, and 5, create definitions in JP1/AJS3 for Cloud Service Applications and run them as service linkage jobs. To design these definitions, the following three considerations are necessary.

- Consider the environment of the connection-destination services and commands to be executed
- Consider the method for managing authentication information corresponding to the commands to be executed
- Consider the linkage processing

(2) Design of service linkage monitoring jobs

The service linkage monitoring jobs of JP1/AJS3 for Cloud Service Applications define how to monitor the cloud services to be monitored. The flow for designing a service linkage monitoring job is as follows.

1. Consider the flow of business operations based on events, where, for example, a business operation is triggered by a change in the particular status of a cloud service, and then decide on the cloud services to be monitored as a custom event job or start condition of JP1/AJS3.
2. Investigate and consider the specifications of the relevant cloud services and the command interfaces that can be linked.
3. Design the processing for connecting to the cloud service.
4. Design the method for managing information for performing authentication with the cloud service.
5. Design the processing for monitoring the cloud service.

Based on the content designed in 3, 4, and 5, create definitions in JP1/AJS3 for Cloud Service Applications and run them as service linkage monitoring jobs. To design these definitions, the following three considerations must be accounted for.

- Consider the environment of the connection-destination services and commands to be executed
- Consider the method for managing authentication information corresponding to the commands to be executed
- Consider the monitoring processing

4.1.2 Consideration according to connection-destination services and command execution environments

You should consider whether to perform connection processing and whether to use common environment variables depending on the connection-destination service.

(1) Whether connection processing is necessary

Depending on the connection-destination service, no processing is required to establish connection or command execution is required, for instance, to enter a user name and password for establishing connection.

The latter case requires defining the cloud service linkage connection information and cloud service linkage authentication information each. For details on these definition items, see [7.1.10 Connection definitions window](#) and [7.1.11 Authentication definitions window](#).

(2) Whether common environment variables are necessary

Check for common environment variables that are used for execution of the commands at the execution host. For details on these definition items, see [7.1.10 Connection definitions window](#).

4.1.3 Considering the method for managing authentication information corresponding to the commands to be executed

Consider the method for managing authentication information corresponding to the interface for the commands to be executed.

If connection processing in [4.1.2 Consideration according to connection-destination services and command execution environments](#) and common environment variables are necessary, see the management methods in (1) and (2). If connection processing is not particularly necessary, see the management method in (3).

(1) Specifying environment variables during command execution

If the command uses environment variable information (for example, account information or access key information) to perform connection, consider the following management methods.

- Registering information in the authentication definition
- Setting the relevant environment variables in **Common environment variable settings** of the connection definition

With these management methods, environment variables are set and operated for every command that is executed.

(2) Specifying arguments for a command

To specify authentication information in arguments (for example, account information or access key information) to perform connection, consider the following management method.

- Registering information in the authentication definition
- Considering the following definition methods depending on the connection method of the cloud service
 - If the following is unnecessary when a command for connection is executed first:
Using **Command line** of **Connection processing** in the connection definition to set authentication information in the argument of the command

- If it is always necessary to specify arguments for the command in the linkage processing:
Using each **Command line** item of the execution definition or monitoring definition to set authentication information in the argument of the command

(3) Performing operations by using the environment settings on the side of the command

On the command's authentication interface, if connection is possible even if you do not perform connection processing by specifying environment variables and argument as in (1) and (2), it is not necessary to define authentication definitions or connection definitions in JP1/AJS3 for Cloud Service Applications.

For example, if the management method exists on the side of the command as in the following, consider using it.

- Using temporary authentication information
This is a method that assigns access permissions to command execution environments, such as virtual machines, by using the functions of the cloud service. If the management destinations of access permissions are unified on the side of the cloud service, it is advantageous as a method where the distributed management of authentication information is not necessary.
- Using long-term authentication information
This is a method that sets authentication information on the execution-destination host of the linkage job in advance, for example, by using the setup processing of the command.

4.1.4 Considering the linkage processing

It is necessary to define the processing for linking to cloud services as execution definitions. To define the processing, design the linkage processing as follows. For details on the definition items, see the description of the Execution definition window in *7. Operation*.

1. In **Execution start processing**, set the command line for executing linkage processing.
2. In **End confirmation processing**, if the command in 1 is asynchronous and does not wait for the end, configure settings so that it waits until the end.
3. In **Post-processing (normal end)**, if it is necessary to collect the results of the executed service, configure the settings.
4. In **Post-processing (abnormal end)**, if it is necessary to suspend service execution if the command execution or end confirmation processing in 1 and 2 end abnormally, configure the settings.

In addition to the aforementioned design, it is necessary to consider the following, taking into account job operation in JP1/AJS3.

- Parameters to be changed dynamically
- Judgment of result
- Designing job output
- Trace information design
- Job output design

The following details these items.

(1) Parameters to be changed dynamically

Parameters that are changed dynamically may be specified for service linkage jobs to be operated. Examples of such parameters include the following.

- File names to be stored in a storage service, file paths to file sources
- Workflow names of workflow services
- Instance names for start or stop of virtual machines of computing services
- Batch names used for batch execution of computing services
- Function names used for server-less code execution services of computing services

Define these items for JP1/AJS3 - View jobs. Define these in JP1/AJS3 - View jobs. Regarding the things to be specified on the side of the job, consider the settings in **Variable settings**.

In addition, design the authentication information used to connect to cloud services in units of job execution. Specify the authentication definition that is used during job definition in JP1/AJS3 - View.

(2) Judgment of result

Consider a judgment condition for the result of a job executed on the host of the connection-destination service. Define these judgment criteria in **End confirmation processing**. Consider whether it is possible to perform judgment based on the standard output of each command.

(3) Designing job output

Consider and design standard output for using the execution result of service linkage jobs for subsequence jobs and what to be output to the result details screen of JP1/AJS3 - View or JP1/AJS3 - Web Console. Define the design content for job output in **Job output processing**.

(4) Trace information design

Consider and design trace information that is checked on the result details screen of JP1/AJS3 - View or JP1/AJS3 - Web Console in the event of an abnormal end of service linkage job execution, or is stored in the log for troubleshooting. Define the design content for trace information in **Trace information settings**.

4.1.5 Considering the monitoring processing

It is necessary to define the monitoring processing of what activities in cloud services are to be checked as events and when the events are determined to be occurring as monitoring definitions. To define the processing, design the monitoring processing as follows. For details on the definition items, see the descriptions of the monitoring definition windows in [7. Operation](#).

1. Set the command line for obtaining the information on the cloud service. Design it so that the information can be output to the standard output as data in JSON format.
2. Design the JMESPath query statement to extract the data to be used for monitoring from the information acquired by the command in 1 (information to be monitored) and store the extracted data.
3. In **Execution result judgment**, choose whether monitoring continues or command execution ends abnormally when the command line executed in 1 ends abnormally.

4. In **Passing information settings**, design whether it is necessary to pass the monitoring information extracted in 2 to the subsequent job in JP1/AJS3 - Manager.

In addition to the aforementioned design, it is necessary to consider the following, taking into account job operation in JP1/AJS3.

- Parameters to be changed dynamically
- Monitoring information design
- Trace information design
- Passing information design

The following details these items.

(1) Parameters to be changed dynamically

Parameters that are changed dynamically may be specified for service linkage monitoring jobs to be operated. Examples of such parameters include the following.

- Object names of storage services to be monitored
- Bucket name of storage services to be monitored
- Storage account name or container name of storage services to be monitored

Define these parameters in JP1/AJS3 - View jobs. Regarding the things to be specified on the side of the job, consider the settings in **Variable settings**.

In addition, design the authentication information used to connect to cloud services in units of job execution. Specify the authentication definition that is used during job definition in JP1/AJS3 - View.

(2) Monitoring information settings

Consider what information in the connection-destination services should be monitored. Define this monitoring information in **Monitoring processing**. Consider whether the JMESPath query statement can be used to extract the standard output (JSON) of the information acquisition command, as well as the result.

At this time, if numerous data items are output by the information acquisition command, there is a possibility of a decrease in the execution performance of service linkage monitoring jobs, large consumption of memory resources, or an abnormal termination of a service linkage monitoring job due to the maximum standard output size being reached. Please consider using the command line options that will output only the information necessary for monitoring.

(3) Trace information design

Trace information for service linkage monitoring jobs has the following two considerations:

First, consider which information from an information acquisition command should be logged when the command is executed at a monitoring interval. Available setting options are the *executed command line* and the *standard error output*. These settings must be considered together with the log sizes because they are output at every monitoring interval. This information is defined in **Trace information settings**.

Second, consider how trace information should be handled when **Abnormal end occurs** is selected for a job if it ends abnormally upon execution of an information acquisition command. When **Monitoring continues** is selected, consider the first design only. Consider and design trace information that is checked on the result details screen of JP1/AJS3 - View or JP1/AJS3 - Web Console in the event of an abnormal end of a job, or is stored in the log for troubleshooting. Define

this information in **Output settings for detailed execution results** and **Log output settings** configured in **Execution result judgment**.

(4) Passing information design

Consider and design the passing information settings so that succeeding jobs receive and use the information obtained after the monitoring condition is met in a service linkage monitoring job. The service linkage monitoring job is executed as a custom event job in JP1/AJS3. Consider what value should be stored in each of the fields, **OBJECT01** to **OBJECT10**, for the passing information name of this custom event job after the monitoring condition is met. Define the design content for passing information in **Passing information settings**.

4.2 Definition flow of a linkage job

The following illustrates the flow of defining a linkage job.

1. Output a service linkage job information file or service linkage monitoring job information file on the Web screen of the JP1/AJS3 for Cloud Service Applications server.
Select service linkage job execution information or service linkage monitoring information to be used when the service linkage information file or service linkage monitoring job information file is output.
2. Execute the `ajscsajobreg` command for registration with JP1/AJS3 - View.
For details on the `ajscsajobreg` command, see *ajscsajobreg (Windows only)* in 8. *Commands*.
3. Start the custom job details definition screen or custom event job details definition screen of JP1/AJS3 - View.
For details on the custom job definition using JP1/AJS3 - View, see the description on the custom job in the *JP1/Automatic Job Management System 3 Linkage Guide*.
4. Enter definition items for the service linkage job on the custom job details definition screen, or for the service linkage monitoring job on the custom event job details definition screen, of JP1/AJS3 - View, and click **OK**.
The definitions of the service linkage job or service linkage monitoring job will be stored in JP1/AJS3.

4.3 Definition items of linkage job information

Define linkage job information on the Web screen of the JP1/AJS3 for Cloud Service Applications server. For details on these definition items, see [7. Operation](#).

This section describes the variables used for definition and notes. Here we provide an explanation of variables used in definitions and notes.

4.3.1 Variables used for the definition of service linkage job information

For a service linkage job, you can define and use information that changes with each job execution as variables.

(1) Types of variables

When defining service linkage job information, you can define and use the following items as variables. For details on specific locations where variables are defined and on definition items for which variables can be used, see [7. Operation](#).

- Variables that store the values specified in custom job definitions
- Variables that store environment variables of the service linkage job execution environment
In JP1/AJS3, you can also store the environment variables that are set at job execution in environment variables of the service linkage job execution environment. For details about environment variables that are set at job execution, see the descriptions of environment variables that are set when jobs are executed from JP1/AJS3 in the *JP1/Automatic Job Management System 3 Command Reference*.
- Variables reserved by the system and available by default
Variables that are automatically set when a service linkage job is executed are variables reserved by the system and available by default.

Variable name	Description
?CSASUUID?	UUID acquired when the service linkage job started
?CSASSTARTDAY?	System date when the service linkage job started
?CSASSTARTTIME?	System time when the service linkage job started

- Variables that store the results of the standard output of the executed command lines
- Variables that store the values of authentication information

(2) Format of variable names

The format of variable names used for service linkage jobs is `?CSAany-character-string?`.

For details about the format that can be specified for service linkage job information, see [7. Operation](#).

(3) How to use variables

When you reference variables in the definition items of the service linkage job information, how to use variables depends on the type of the variable.

- Variables that store the values specified in custom job definitions
- Variables that store environment variables of the service linkage job execution environment

- Variables that are reserved by the system and available by default
- Variables that store the values of authentication information
Specify the variable name as is in the format of `?CSAany-character-string?`.
- Variables that store the results of the standard output of the executed command lines
Specify in the format of `?CSAany-character-string [any-number] ?`. For *any-number*, specify the value of "number-of-lines-1" in the result of standard output. For example, to reference the first line of the results of standard output, specify `?CSAany-character-string [0] ?`. To reference the 15th line, specify `?CSAany-character-string [14] ?`. Do not add a leading zero to the number.

(4) Resolution of variables

The value of a variable is resolved when the service linkage job is executed. Note that if the variable is undefined or if the value of *any-number* is invalid when referencing the result of standard output, the variable portion is resolved as an empty character string.

4.3.2 Variables used for the definition of service linkage monitoring job information

For a service linkage monitoring job, you can define and use information that changes with each job execution as variables.

(1) Types of variables

When defining service linkage monitoring job information, you can define and use the following items as variables. For details on specific locations where variables are defined and on definition items for which variables can be used, see [7. Operation](#).

- Variables that store the values specified in custom event job definitions
- Variables that store environment variables of the service linkage monitoring job execution environment
These variables work by reading the environment variables configured for daemons corresponding to the types of linked monitoring jobs. The daemons are started at startup of JP1/AJS3 services, and therefore system environment variables and other variables when such services are started are available.
- Variables reserved by the system and available by default
Variables that are automatically set when a service linkage monitoring job is executed are variables reserved by the system and available by default.

Variable name	Description
<code>?CSASUUID?</code>	UUID acquired when the service linkage monitoring job execution started
<code>?CSASSTARTDAY?</code>	System date when the service linkage monitoring job execution started
<code>?CSASSTARTTIME?</code>	System time when the service linkage monitoring job execution started

- Variables that store the results obtained by extracting the standard output (JSON) of the executed command lines in the JMESPath query syntax
Based on the extracted information, only the result that fulfills the condition for monitoring completion will be saved in the corresponding variable.
- Variables that store the values of authentication information

(2) Format of variable names

The format of variable names used for service linkage monitoring jobs is `?CSAany-character-string?`.

For details about the format that can be specified for service linkage monitoring job information, see [7. Operation](#).

(3) How to use variables

When you reference variables in the definition items of the service linkage monitoring job information, specify all the variables in the formant of `?CSAany-character-string?` as they are.

(4) Resolution of variables

The value of a variable is resolved when the service linkage monitoring job is executed. Note that if the variable is undefined, the variable portion is resolved as an empty character string.

4.3.3 Escaping a command line for cloud service linkage information

When specifying symbol characters that must be escaped in a command line, the method for specifying escape characters differs depending on the OS. In JP1/AJS3 for Cloud Service Applications, by using the functionality described below, you can escape character strings according to the OS of the job execution host.

Use the following methods to specify escaping:

- Specify in the form of `"@CSA (character-string-to-escape) ASC@"` by enclosing the portion of the command line that you want to escape with `"@CSA ("` (escape-start character) and `") ASC@"` (escape-end character). For example, to escape the character string `"a \ a"`, specify `"@CSA(a \ a)ASC@"`.
- The *character-string-to-escape* is specified as a variable, and is escaped by using the result of resolving the variable.
- Characters from the escape-start character are ignored until the escape-end character appears.

The following shows how to escape in Windows and Linux.

<In Windows>

- If the number of consecutive backslashes (`\`) before the quotation mark (`"`) is n (one or more), set the number of backslashes (`\`) as 2 times n .
- Replace the quotation mark (`"`) with the symbol (`\ "`).
- If the number of consecutive backslashes (`\`) at the end is n (one or more), set the number of backslashes (`\`) as 2 times n .
- Enclose the entire character string that you want to escape with quotation marks (`"`).

<In Linux>

- Replace the backquote (```) with the symbol (`\ ``).
- If there is no apostrophe (`'`), enclose the entire character string that you want to escape with apostrophes (`'`).
- If the string contains apostrophes (`'`), change it by performing the following:
 - (1) Divide the value by using an apostrophe (`'`).

- (2) Replace the apostrophe (') with a backslash (\), and then enclose each of other divided character string with apostrophes (').
- (3) Concatenate all character strings that were divided in (1) and edited in (2).

4.3.4 Notes on the definitions of linkage job information

(1) About definitions used for job execution

The service linkage job definitions, service linkage monitoring job definitions, and authentication definitions defined in JP1/AJS3 for Cloud Service Applications are used by JP1/AJS3 as service linkage jobs or service linkage monitoring jobs in JP1/AJS3. Therefore, job execution of JP1/AJS3 may be affected if the definition of service linkage job information or service linkage monitoring job information is updated or deleted.

Whether or not the job execution of JP1/AJS3 is affected is displayed on the Web screen of JP1/AJS3 for Cloud Service Applications as follows.

- When updating or deleting the service linkage job definition, service linkage monitoring job definition, or authentication definition used for a job that has once been executed, the message KNBB2407-Q or KNBB2408-Q is displayed in a dialog.
- When editing each definition on the Web screen of the JP1/AJS3 for Cloud Service Applications, the upper part of the screen shows a message !This is a definition that has a job execution history.

Note that the period of time when such dialog or message is displayed depends on the value specified for `USED_DEF_LIMIT` in the environment setting file. For details on the environment setting file, see [3.4.1 Details of setting items of the environment setting file \(ajs3csaweb.conf\)](#).

For service linkage monitoring jobs, note that:

- Regarding authentication definition, the history information will be updated after the monitoring starts or when the monitoring processing runs for each monitoring interval. Therefore, the timing for displaying a message is different from other definitions.

In addition, when creating new service-linkage job definitions, service-linkage monitoring job definitions, or authentication definitions, if you perform registration by using a definition name that has previously been executed, even if the job has not executed even once, the aforementioned display processing is performed.

To check the details of a user's job in JP1/AJS3, use one of the following methods:

- Check the unit name and host name of the job by referencing server job logs of JP1/AJS3 for Cloud Service Applications. For details about server job logs, see [9.2.4 Server Job Logs](#).
- From the content of the unit definitions output by the `ajsprint` command or by JP1/AJS3 - Definition Assistant in JP1/AJS3, search for and check the service linkage jobs or service linkage monitoring jobs. For details about unit definition parameters, see [4.5 Unit definition parameters of service linkage jobs](#) and [4.6 Unit definition parameters of service linkage monitoring jobs](#). For details about how to check the name of service linkage jobs and service linkage monitoring jobs, see the description of the `ajscsajoblist` (Windows only) in [8. Commands](#).

(2) About definitions used in the service linkage job definitions

For service linkage job definitions, the connection definition and execution definition are specified to execute a job as the service linkage job. Therefore, job execution of JP1/AJS3 may be affected if the connection definition and execution definition are updated or deleted.

Whether or not the service linkage job definitions are affected is shown on the Web screen of JP1/AJS3 for Cloud Service Applications as follows.

- When updating or deleting the connection definition or execution definition used for the service linkage job definitions, the message KNBB2409-Q or KNBB2410-Q is displayed in a dialog.
- When you edit a connection definition on the Web screen of the JP1/AJS3 for Cloud Service Applications, the upper part of the screen shows a message stating !This is the definition used in the service linkage job definition or the service linkage monitoring job definition. When you edit an execution definition, it shows a message stating !This is the definition used in the service linkage job definition.

(3) About definitions used in the service linkage monitoring job definitions

For service linkage monitoring job definitions, the connection definition and monitoring definition are specified to execute a job as the service linkage job. Therefore, job execution of JP1/AJS3 may be affected if the connection definition and monitoring definition are updated or deleted.

Whether or not the service linkage monitoring job definitions are affected is shown on the Web screen of JP1/AJS3 for Cloud Service Applications as follows.

- When updating or deleting the connection definition or monitoring definition used for the service linkage monitoring job definitions, the message KNBB2409-Q or KNBB2410-Q is displayed in a dialog.
- When you edit a connection definition on the Web screen of the JP1/AJS3 for Cloud Service Applications, the upper part of the screen shows a message stating !This is the definition used in the service linkage job definition or the service linkage monitoring job definition. When you edit an monitoring definition, it shows a message stating !This is the definition used in the service linkage monitoring job definition.

(4) About handling of authentication information

Information that is registered with Protect specified in the authentication definitions is stored in the database file (AJSCSA.db) and backup file (AJSCSA.db.back) in the data directory in a non-plain-text, protected state.

No authentication information is output to a log file, the standard output or standard error output of a job, nor the detailed execution results screen of JP1/AJS3 - View and JP1/AJS3 - Web Console.

Consider the notes below while taking into account the operations above when building an environment and designing security measures.

- Communication is performed by using protected non-plain-text information. However, authentication information is included in communication data. For this reason, we recommend that you build an SSL communication environment, unless your environment has no security risks, such as the risk of data being read on the communication path.
- JP1/AJS3 for Cloud Service Applications does not output protected authentication information to the standard output, standard error output, logs, and the detailed execution results screen of JP1/AJS3 - View and JP1/AJS3 - Web Console, but may output authentication information to the command line used for definition. Before specifying definitions, check and verify the specifications of the command lines to be used.

(5) Other notes

- To check with the changed service linkage job information about whether the job has been executed, take either of the following methods.

- Open the service linkage job log file on the job execution host, and check if the command line with changed details has been output on the CLI.
- When details have been changed in the standard error output or standard output of the service linkage job, check the execution result details check screen of JP1/AJS3 - View and JP1/AJS3 - Web Console or the data in the standard output file.
- To check with the changed service linkage monitoring job information about whether the job has been executed, take either of the following methods.
 - Open the log file for a monitoring job on the job execution host, and check if the command line with changed details has been output on the CLI.
 - When execution result setting details have been changed on a service linkage monitoring job, check the execution result details check screen of JP1/AJS3 - View and JP1/AJS3 - Web Console.

4.4 How to define linkage jobs

Define linkage jobs in JP1/AJS3.

This section describes how to define linkage jobs.

4.4.1 Details of the definition of linkage jobs

(1) Service linkage jobs

Register service linkage jobs as custom jobs of JP1/AJS3. For details on custom jobs, see the description on the custom job in the *JP1/Automatic Job Management System 3 Linkage Guide*.

(2) Service linkage monitoring jobs

Register service linkage monitoring jobs as custom event jobs of JP1/AJS3.

4.4.2 Place where linkage jobs can be defined

(1) Service linkage jobs

Service linkage jobs can be defined as unit definitions in the following places.

- root jobnet
- nested jobnet group
- root job group[#]
- job group[#]

#

Service linkage jobs cannot be defined from the New menu item of JP1/AJS3 - View, but can be defined by the following methods.

- With the service linkage job existing on the clip board when using JP1/AJS3 - View, paste the job under the root job group or job group.
- In the unit definition file, describe the definitions of the service linkage job under the root job group or job group, and execute the `ajsdefine` command.

Service linkage jobs cannot be defined any place other than the above.

(2) Service linkage monitoring jobs

Service linkage monitoring jobs can be defined as unit definitions in the following places.

- root jobnet
- nested jobnet
- root job group[#]

- job group[#]
- start condition

#

Service linkage monitoring jobs cannot be defined from the New menu item of JP1/AJS3 - View, but can be defined by the following methods.

- With the service linkage monitoring job existing on the clip board when using JP1/AJS3 - View, paste the job under the root job group or job group.
- In the unit definition file, describe the definitions of the service linkage monitoring job under the root job group or job group, and execute the `ajsdefine` command.

Service linkage monitoring jobs cannot be defined in any place other than the above.

4.4.3 Definition items of service linkage jobs

There are following two types of definition items of service linkage jobs.

- Items to be defined on the Custom job unit definition screen
- Items to be defined on the Custom job details definition screen

(1) Items to be defined on the Custom job unit definition screen

The following table shows the items to be defined on the Custom job unit definition screen.

Table 4–1: Custom job unit definition items

Definition items	Comment
Unit name	--
Comment	--
Exec-agent	--
Priority	--
Standard output	--
Standard error	--
End judgment (Rule)	--
End judgment (Warning)	Define the value according to the return code of the service linkage job.
End judgment (Abnormal)	Define the value according to the return code of the service linkage job.
Retry on abnormal end	--
Return code (Less than or equal to)	--
Return code (Greater than or equal to)	--
Maximum retry times	--
Retry interval	--

Definition items	Comment
User name	--
Hold	--
Type	--
Set timeout period	Specify this item according to the details of service linkage job.
Timeout period	Specify this item according to the details of service linkage job.
Delayed end	--
Time assumed as delay	--
Owner	--
JP1 resource group	--
Executed by	--

Legend:

--: Same as those set for the existing job definition

(2) Items to be defined on the Custom job details definition screen

The following table shows the items to be defined on the Custom job details definition screen.

Table 4–2: Custom job details definition items

Definition items	Comment	Whether to specify macro variables
Authentication definition name	Specify the name of service linkage authentication information to be applied.	Y
Variable definition items		Y

Legend:

Y: Macro variables can be specified.

The result of passing on of macro variables can be checked with JP1/AJS3 - View or the `ajsshows` command.

4.4.4 Definition items of service linkage monitoring jobs

There are the following two types of definition items of service linkage monitoring jobs.

- Items to be defined on the Custom event job unit definition screen
- Items to be defined on the Custom event job details definition screen

(1) Items to be defined on the Custom event job unit definition screen

The following table shows the items to be defined on the Custom event job unit definition screen.

Table 4–3: Custom event job unit definition items

Definition items	Comment
Unit name	--

Definition items	Comment
Comment	--
Exec-agent	--
Hold	--
Type	--
Set timeout period	--
Timeout period	--
Status after close	--
Delayed end	--
Time assumed as delay	--
Owner	--
JP1 resource group	--
Executed by	Specify the type of the user for the command executed by the monitoring job.
Passing Info button	For details about the information that can be passed to, see the description about the passing information of monitoring jobs for each monitored service in <i>Chapter 6</i> .
Details button	Starts the Custom event job details definition screen on the monitoring job for each monitored service.

Legend:

--: Same as those set for the existing job definition

(2) Items to be defined on the Custom event job details definition screen

This section describes the items to be defined on the Custom event job details definition screen.

Although a details definition screen to be started is specific to a monitoring job for each monitored service, it also has definition items common to every details definition screen. The following table shows the common definition items.

Table 4–4: Common details definition items for service linkage monitoring jobs

Definition items	Comment	Whether to specify macro variables
Authentication definition name	Specify the name of service linkage authentication information to be applied.	Y
Variable definition items		Y

Legend:

Y: Macro variables can be specified.

The following table shows the items that can be defined for each monitored service.

Table 4–5: Details definition items for service linkage objects monitoring jobs

Definition items	Comment	Whether to specify macro variables
Name of the object to be monitored	Specify the name of the object to be monitored.	Y
Monitoring options	Select either Create , Delete , or Update .	--

Definition items	Comment	Whether to specify macro variables
Monitoring options	For create monitoring and delete monitoring, specify the behavior option where the monitoring condition is met.	--
Monitoring interval	Specify a monitoring interval in seconds.	N

Legend:

Y: Macro variables can be specified.

N: Macro variables cannot be specified.

--: It is not a text box. (Text itself cannot be entered.)

You can check the passing results of macro variables in JP1/AJS3 - View or with the `ajsshows` command.

4.4.5 Icon of linkage jobs

For the icon of linkage jobs, you can use either the icon of a custom job or custom event job, or the default icon installed in JP1/AJS3 - View.

The format of the custom job or custom event job icon is the same as that of the gif file for icons used for registering a custom PC job or custom UNIX job. For details, see the description on the gif file format for icons in the *JP1/Automatic Job Management System 3 Linkage Guide*.



Note

The icon of linkage jobs can be displayed only with JP1/AJS3 - View. JP1/AJS3 - Web Console displays the same icon as those of other standard custom jobs or custom event jobs.

4.4.6 Operation of service linkage jobs

This section describes registration, listing, and deletion of service linkage jobs.

(1) Registration of service linkage jobs

The following shows the procedure for registering a service linkage job.

1. Export a service linkage definition file from the JP1/AJS3 for Cloud Service Applications server, and place the file in a desired folder on the host with JP1/AJS3 - View installed.
2. Start the command prompt on the host with JP1/AJS3 - View installed.
3. Specify the path to the service linkage definition file, custom job name, and the path to the icon file (when using the custom job icon) for arguments, and execute the `ajscsajobreg` command.
For details on the `ajscsajobreg` command, see *ajscsajobreg (Windows only)* in 8. *Commands*.
4. Restart JP1/AJS3 - View.
The registered information will be enabled after restart.
5. Click the **Custom jobs** tab in the Jobnet Editor window, and check that the icon has been added.
Place the mouse cursor over the icon, and the custom job name appears in a tool tip.

(2) Listing of service linkage jobs

The following shows the procedure for listing service linkage jobs.

1. Start the command prompt on the host with JP1/AJS3 - View installed.
2. Execute the `ajscsajoblist` command.
For details on the `ajscsajoblist` command, see *ajscsajoblist (Windows only)* in 8. *Commands*.

(3) Deletion of service linkage jobs

The following shows the procedure for deleting a service linkage job.

1. Start the command prompt on the host with JP1/AJS3 - View installed.
2. Specify a custom job name you want to delete for an argument, and execute the `ajscsajobdel` command.
For details on the `ajscsajobdel` command, see *ajscsajobdel (Windows only)* in 8. *Commands*.
3. Restart JP1/AJS3 - View.
The registered information will be enabled after restart.
4. Click the **Custom jobs** tab in the Jobnet Editor window, and check that the icon has been deleted.

(4) When using a different service linkage job for each JP1 user

You can switch the service linkage job displayed on the Jobnet Editor window of JP1/AJS3 - View based on each JP1 user by dividing folders containing custom job registration information and service linkage job specific information for each JP1 user.

The following shows the procedure for using a different service linkage job for each JP1 user.

1. Create an `extend` folder immediately under the custom job registration information folder *data-folder-of-JP1/AJS3 - View\custom.dir*. Then, immediately under this folder, create a folder specified in the user specified option file `jajsCustomJobDirectory`.
2. Create a `extend` folder immediately under the folder storing service linkage job specific information *data-folder-of-JP1/AJS3 - View\csadef*. Then, immediately under this folder, create a folder specified in the user specified option file `jajsCustomJobDirectory`.
3. Grant the read and write privileges to the folder created in the steps 1 and 2.
4. For the environment variable `AJS_CSA_VIEW_CUSTOMJOBDIR`, specify the folder name that is specified for `jajsCustomJobDirectory` in the user specified option file.
If no folder name is specified for the environment variable or if the specified folder does not exist, the default folder (custom job registration information folder: *data-folder-of-JP1/AJS3 - View\custom.dir*, and the folder storing service linkage job specific information: *data-folder-of-JP1/AJS3 - View\csadef*) is used for operation.
5. Operate the service linkage jobs used by the JP1 user by following the procedures for registering, listing, and deleting service linkage jobs.

4.4.7 Operation of service linkage monitoring jobs

This section describes registration, listing, and deletion of service linkage monitoring jobs.

(1) Registration of service linkage monitoring jobs

The following shows the procedure for registering a service linkage monitoring job.

1. Export a service linkage monitoring definition information file from the JP1/AJS3 for Cloud Service Applications server, and place the file in a desired folder on the host with JP1/AJS3 - View installed.
2. Start the command prompt on the host with JP1/AJS3 - View installed.
3. Specify the path to the service linkage monitoring definition information file, the custom event job name, and the path to the icon file (when using the custom event job icon) for arguments, and execute the `ajscsajobreg` command.
For details on the `ajscsajobreg` command, see *ajscsajobreg (Windows only)* in 8. *Commands*.
4. Restart JP1/AJS3 - View.
The registered information will be enabled after restarting.
5. Click the **Custom Events** tab in the Jobnet Editor window, and check that the icon has been added.
Place the mouse cursor over the icon, and the custom event job name appears in the tool tip.

(2) Listing of service linkage monitoring jobs

The following shows the procedure for listing service linkage monitoring jobs.

1. Start the command prompt on the host with JP1/AJS3 - View installed.
2. Execute the `ajscsajoblist` command with the `-m` option specified.
For details on the `ajscsajoblist` command, see *ajscsajoblist (Windows only)* in 8. *Commands*.

(3) Deletion of service linkage monitoring jobs

The following shows the procedure for deleting a service linkage monitoring job.

1. Start the command prompt on the host with JP1/AJS3 - View installed.
2. Specify the name of the custom event job you want to delete for an argument, and execute the `ajscsajobdel` command with the `-m` option specified.
For details on the `ajscsajobdel` command, see *ajscsajobdel (Windows only)* in 8. *Commands*.
3. Restart JP1/AJS3 - View.
The registered information will be enabled after restarting.
4. Click the **Custom Events** tab in the Jobnet Editor window, and check that the icon has been deleted for that job.

(4) When using a different service linkage monitoring job for each JP1 user

You can switch the service linkage monitoring job displayed on the Jobnet Editor window of JP1/AJS3 - View based on each JP1 user by dividing folders containing custom event job registration information and service linkage monitoring job specific information for each JP1 user.

The following shows the procedure for using a different service linkage monitoring job for each JP1 user.

1. Create an `extend` folder immediately under the custom event job registration information folder *data-folder-of-JP1/AJS3 - View\customevent.dir*. Then, immediately under this folder, create a folder specified in the user specified option file `jajsCustomEventJobDirectory`.
2. Create an `extend` folder immediately under the folder storing service linkage monitoring job specific information *data-folder-of-JP1/AJS3 - View\csadef\customevent*. Then, immediately under this folder, create a folder specified in the user specified option file `jajsCustomEventJobDirectory`.
3. Grant the read and write privileges to the folder created in the steps 1 and 2.
4. For the environment variable `AJS_CSA_VIEW_CUSTOMEVJOBDIR`, specify the folder name that is specified for `jajsCustomEventJobDirectory` in the user specified option file.
If no folder name is specified for the environment variable or if the specified folder does not exist, the default folder (custom event job registration information folder: *data-folder-of-JP1/AJS3 - View\customevent.dir*, and the folder storing service linkage monitoring job specific information: *data-folder-of-JP1/AJS3 - View\csadef\customevent*) are used for operation.
5. Operate the service linkage monitoring jobs used by the JP1 user by following the procedures for registering, listing, and deleting service linkage monitoring jobs.

4.4.8 Notes on linkage jobs

(1) Service linkage job

The service linkage jobs registered by the procedure described in [4.4.6 Operation of service linkage jobs](#) are displayed in the Register Custom Job dialog box of JP1/AJS3 - View.

The following shows notes on operating service linkage jobs using this dialog box.

- Do not change service linkage jobs in the Register Custom Job dialog box.
- If a service linkage job is deleted from the Register Custom Job dialog box, unnecessary files remain undeleted. Delete manually the files shown in the table below.

Table 4–6: Files of service linkage jobs that need manual deletion

Custom job types	Files to be deleted
Common	<i>JP1/AJS3 - View-installation-folder</i> ^{#1} \image\custom\CUSTOM_PC_CSA <i>custom-job-name</i> .gif
	%ALLUSERSPROFILE% ^{#2} \Hitachi\JP1\JP1_DEFAULT\JP1AJS2V\csadef\i>custom-job-name.json
	%ALLUSERSPROFILE% ^{#2} \Hitachi\JP1\JP1_DEFAULT\JP1AJS2V\log\i>custom-job-name{1 2}.log

#1

By default, the JP1/AJS3-installation-folder is *system-drive*\Program Files (x86)\HITACHI\JP1AJS2V.

#2

By default, %ALLUSERSPROFILE% is *system-drive*\ProgramData.

4.5 Unit definition parameters of service linkage jobs

This section describes the definition parameters of service linkage jobs. For details on the unit definition parameters of JP1/AJS, see the description on the creation of information definition files in the manual *JP1/Automatic Job Management System 3 Command Reference*.

4.5.1 Description format of unit definition parameters of service linkage jobs

The following shows the description format of the unit definition parameters of a service linkage job.

```
{
  ty={cpj|rcpj};
  cm="comment";
  cty="CSAservice-linkage-job-name";
  sc="$JP1AJS2_JPOEXEPATH$/ajscsaexec";
  env="AJS_CSA_AUTHINFNAME=authentication-definition-name";
  env="AJS_CSA_DEFINFNAME=service-linkage-job-definition-name";
  env="AJS_CSA_ENV_variable-value=value-to-be-input-in-the-custom-job-definition";
  so="standard-output-file-name";
  se="standard-error-output-file-name";
  etm=n;
  fd=Required-execution-time;
  pr=n;
  ex="execution-agent-name";
  un="execution-user-name";
  jd={nm|ab|cod};
  wth=n;
  tho=n;
  abr={y|n};
  rjs=lower-limit-of-automatic-retry-return-code;
  rje=upper-limit-of-automatic-retry-return-code;
  rec=maximum-number-of-retry-times;
  rei=retry-interval;
  ha={y|n};
  eu={ent|def};
}
```

4.5.2 Details of the unit definition parameters of service linkage jobs

This section describes the details of the unit definition parameters of service linkage jobs. For parameters other than those listed below, see the description on the creation of information definition files in the manual *JP1/Automatic Job Management System 3 Command Reference*.

```
cty="CSAservice-linkage-job-name";
```

This is a parameter for specifying a custom job class name. For a service linkage job of JP1/AJS3 for Cloud Service Applications, specify a character string with a service linkage job name added at the end of CSA, as the custom job class name.

```
sc="$JP1AJS2_JPOEXEPATH$/ajscsaexec";
```

This is a parameter for specifying a script file name. For a service linkage job of JP1/AJS3 for Cloud Service Applications, this parameter is fixed to \$JP1AJS2_JPOEXEPATH\$/ajscsaexec.

```
env="AJS_CSA_AUTHINFNAME=authentication-definition-name";
```

This is a parameter for specifying the environment variable AJS_CSA_AUTHINFNAME. When authentication definition is required for executing a service linkage job of JP1/AJS3 for Cloud Service Applications, specify an authentication definition name.

```
env="AJS_CSA_DEFINFNAME=service-linkage-job-definition-name";
```

This is a parameter for specifying the environment variable AJS_CSA_DEFINFNAME. Specify a service linkage job definition name of JP1/AJS3 for Cloud Service Applications. This item is required.

```
env="AJS_CSA_ENV_variable-value=value-to-be-input-in-the-custom-job-definition";
```

This is a parameter for specifying the environment variable AJS_CSA_ENV_*variable-value*. Specify a value to be input in the custom job definition. Specify the name that has been defined in the service linkage definition file, with the *variable-value* in the environment variable key name specified with an integer between 0 and 10.

4.6 Unit definition parameters of service linkage monitoring jobs

This section describes the unit definition parameters of service linkage monitoring jobs. For details on the unit definition parameters of JP1/AJS, see the description on the creation of information definition files in the manual *JP1/Automatic Job Management System 3 Command Reference*.

4.6.1 Description format of unit definition parameters of service linkage monitoring jobs

The following shows the description format of the unit definition parameters of a service linkage monitoring job.

```
{
  ty={cewj|rcewj};
  cm="comment";
  cety="CE_service-linkage-monitoring-job-type_monitoring-job-name";
  jpoif=macro-variable-name:passing-information-name;
  cprm="definition-parameter";
  etm=n;
  fd=required-execution-time;
  ex="execution-agent-name";
  ha={y|n};
  eu={ent|def};
  ets={kl|nr|wr|an};
  mm={and|or};
  nmg={y|n};
  eun=name-of-the-unit-whose-end-is-being-waited-for;
  ega={exec|execdefer|none};
  uem={y|n};
}
```

4.6.2 Details of the unit definition parameters of service linkage monitoring jobs

This section describes the details of the unit definition parameters of service linkage monitoring jobs. For parameters other than those listed below, see the description on the creation of information definition files in the manual *JP1/Automatic Job Management System 3 Command Reference*.

`cety="CE_service-linkage-monitoring-job-type_monitoring-job-name";`

This is a parameter for defining the information used to identify which program is linked with the custom event job. In a service linkage monitoring job of JP1/AJS3 for Cloud Service Applications, you can define an identifier that denotes the type of the service linkage monitoring job listed in the following table.

Table 4–7: List of service linkage monitoring job types that can be specified

Type of monitoring job	Value to be specified for service linkage monitoring job type
Service linkage objects monitoring job	COBM

Specify a string that begins with `CE_`, followed by the job type listed in the above table, like `CE_service-linkage-monitoring-job-type_`, and followed by a monitoring job name.

```
jpoi f="macro-variable-name:passing-information-name";
```

For specifications such as macro variable names and the maximum allowed sizes of parameters, see the description on the creation of information definition files in the manual *JP1/Automatic Job Management System 3 Command Reference*.

The values available for the name of passing information are CMTMOUT and OBJECT01 to OBJECT10. OBJECT01 to OBJECT10 will store the value configured in the monitoring definition. For details, see the description about the passing information of monitoring jobs for each monitored service in *Chapter 6*.

```
cprm="definition-parameter";
```

Different monitoring job types have different definitions. The following table shows the format and parameter value for each type.

Table 4–8: Definition parameters of service linkage objects monitoring jobs

No.	Item	Format#1	Value#1, #2
1	Authentication definition name	AJS_CSA_AUTHINFNAME= <i>value</i>	Specify any character string of between 0 and 64 bytes. Optional.
2	Monitoring job name	AJS_CSA_MONDEFINFNAME= <i>value</i>	Specify any character string of between 2 and 31 bytes.
3	Parameter (optional definition item)	AJS_CSA_ENV_variable= <i>value</i>	Specify any character string of between 0 and 12,000 bytes. You can define up to 10 instances of this parameter. Optional. Note that the <i>variable-value</i> part can accept a character string consisting of A to Z and 0 to 9 within 58 bytes.
4	Name of the object to be monitored	AJS_CSA_OBJWF= <i>value</i>	Specify any character string of between 1 and 3,072 bytes.
5	Monitoring options	AJS_CSA_OBJWC= <i>value</i>	Specify one of the following characters strings: <ul style="list-style-type: none"> c: Monitors creation of an object. d: Monitors deletion of an object. u: Monitors object updates. These character strings can be specified together and concatenated to create a string of maximum of 3 bytes. Example: cd: Monitors creation and deletion. If multiple character strings are specified, their order does not matter but each character string can be used only once.
6	Monitoring interval	AJS_CSA_OBJWI= <i>value</i>	Specify a numeric value from 10 to 600 of between 2 and 3 bytes (the unit is second). Any 0s that precede the value are ignored.

No.	Item	Format#1	Value#1, #2
7	Operation settings during creation monitoring	AJS_CSA_OBJWCO= <i>value</i>	<p>Specify either of the following character strings:</p> <ul style="list-style-type: none"> • <i>y</i>: Indicates that the monitoring condition is considered to be met if an object already exists when monitoring is started. • <i>n</i>: Indicates that the monitoring condition is considered to be met if an object is detected after monitoring is started. <p>This option is independent of what is specified in the Monitoring options parameter. (An error does not occur if this option is enabled when a value other than <i>c</i> is specified in the Monitoring options parameter.) Optional. If omitted, this parameter assumes <i>n</i>.</p>
8	Operation settings during deletion monitoring	AJS_CSA_OBJWDO= <i>value</i>	<p>Specify either of the following character strings:</p> <ul style="list-style-type: none"> • <i>y</i>: Indicates that the monitoring condition is considered to be met if an object does not exist when monitoring is started. • <i>n</i>: Indicates that the monitoring condition is considered to be met if deletion is detected after monitoring is started. <p>This option is independent of what is specified in the Monitoring options parameter. (An error does not occur if this option is enabled when a value other than <i>d</i> is specified in the Monitoring options parameter.) Optional. If omitted, this parameter assumes <i>n</i>.</p>

#1

If a particular format is specified twice (the first and second ones have the same value in their left-hand side), the value of the second one (defined later) has the precedence over the first.

#2

An optional item can be omitted by:

- Omitting the entire string in the Format column
- Omitting only the *value* part of the string in the Format column

Note that if the value specified for the definition parameter in the above table is invalid, an error is detected when the monitoring job is executed, not when the definition is registered using `ajsdefine`.

5

Management operation of service linkage jobs

This chapter describes a procedure for executing in JP1/AJS3 a service linkage job defined on JP1/AJS3 for Cloud Service Applications.

5.1 Execution of service linkage jobs

Service linkage jobs are executed using information defined on the JP1/AJS3 for Cloud Service Applications server and information of the custom job definition executed from JP1/AJS3 - Manager. Obtain service linkage job execution information from the defined JP1/AJS3 for Cloud Service Applications server.

A service linkage job is executed in the order shown below based on the definition on the JP1/AJS3 for Cloud Service Applications server.

Connection definitions (Connection processing)

When connection processing is defined in the connection definitions, the processing for connecting to the cloud service runs in accordance with the information defined in **Execution command settings**, **Execution result judgment (execution definition)**, and **Trace information settings (execution definition)**.

When the connection processing result is "Normal", the processing is executed according to the execution definitions.

Execution definitions

1. The processing is executed according to the execution start processing of execution definitions.

When the execution result is "Normal", the processing is executed according to the definitions of the end confirmation processing or post processing (when ended normally).

When the execution result is "Abnormal", the processing is executed according to the post-processing definitions (when ended abnormally). When there is no of post-processing definition (when ended abnormally), job output processing is executed.

2. The processing is executed according to the definitions of the end confirmation processing of the execution definitions.

When the execution result is "Normal", processing is executed according to the post-processing definitions (when ended normally) or job output processing definitions.

When the execution result is "Abnormal", processing is executed according to the definitions of the post processing (when ended abnormally). When there is no definition of post processing (when ended abnormally), the job output processing is executed.

3. When the conditions below are met, processing is executed according to the definitions of the post processing (when ended normally).

- Post processing (when ended abnormally) is defined in the execution definitions.

- The execution results of the execution start processing or end confirmation processing are "Normal".

4. When the conditions below are met, processing is executed according to the definitions of the post processing (when ended abnormally).

- Post processing (when ended abnormally) is defined in the execution definitions.

- The execution results of the execution start processing or end confirmation processing are "Normal".

5. When the output processing of a job is defined in the execution definitions, the output processing to the job standard output and job standard error output is executed according to the definitions.

This output processing is executed regardless of the results of the execution start processing, end confirmation processing, post processing (when ended normally), and post processing (when ended abnormally).

Connection definitions (Connection termination processing)

When connection termination processing is defined in the connection definitions, the processing for termination for the cloud service runs in accordance with the information defined in **Execution command settings**, **Execution result judgment (execution definition)**, and **Trace information settings (execution definition)**.

Note that this processing is not executed if the connection processing has failed with an error.

Even if the execution result of the execution definitions is "Abnormal", if the connection result is normal or no connection processing is defined, this processing is executed.

5.2 Details of service linkage jobs

This section describes the details of service linkage jobs.

5.2.1 Status of service linkage jobs

The following describes the statuses of service linkage jobs.

(1) When there does not exist a file on the command line defined on the JP1/AJS3 for Cloud Service Applications server

The service linkage job will end with any return code other than 0.

If there does not exist an "execution file name" or "script file name", a standard JP1/AJS job fails to start. However, a service linkage job does not fail to start even if no file exists on the command line defined on the JP1/AJS3 for Cloud Service Applications server.

(2) Statuses of service linkage jobs and cloud services

In a service linkage job, multiple commands are executed. The "Running" status of the service linkage job that can be checked with JP1/AJS3 may differ from the status of "Running" on the cloud service, depending on when the command is executed.

5.2.2 Environment variables for command execution

The environment variables set for command execution from a service linkage job are enabled according to the priority shown below (1 indicates the highest priority).

- For Windows
 1. Environment variables specified for individual commands
 2. Environment variables specified for environment variables common across the system
 3. Environment variables set for the service linkage job process
(Environment variables set by job execution of JP1/AJS3 and environment variables set by a service linkage job)
- For Linux
 1. Definitions in the system login script
 2. Environment variables specified for individual commands
 3. Environment variables specified for environment variables common across the system
 4. Environment variables set for the service linkage job process
(Environment variables set by job execution of JP1/AJS3 and environment variables set by a service linkage job)

5.2.3 Execution results of service linkage jobs

Execution results of service linkage jobs are output to the standard output and standard error output according to the service linkage execution information. With no information defined, execution results are not output.

The following shows how to output character strings that are defined in the output processing of a job on the JP1/AJS3 for Cloud Service Applications server.

- Standard output
Output without a line break added
- Standard error output
Output with a line break added

When defining service linkage execution information, define information for checking the status on the cloud service side during execution of a service linkage job.

5.2.4 Killing of service linkage jobs

The following table shows the operation when a service linkage job is killed and when the timeout time is reached.

Table 5–1: Operation when a service linkage job is forcibly terminated

Target		Status
Manager	Job on the scheduler service	The status of the service linkage job turns to "kill".
Execution destination (Agent)	Service linkage job	The system forcibly terminates the process of the service linkage job execution program.
	Command	The command process continues operating.
Linked cloud service		The status remains as it was before the forced termination of the service linkage job.

Depending on when killing occurs, the status of a request to the linked cloud service may be unknown. Because of this, check the execution status of the job on the job execution destination and the status of linked cloud service, and take actions as needed.

The following describes how to take actions.

Actions on the service linkage job execution host

When there are unnecessary files on the job execution host, delete them as needed.

The command executed by the service linkage job may still remain running. Therefore, check the command execution status on the job execution host by following the steps below, and forcibly terminate it.

1. Find the process ID of the command from the log of the execution program of the service linkage job.
2. Check the command execution status from the process ID and execution file name by using, for instance, an OS command.

Actions to the linked cloud service

Stop the cloud service as needed because a server-less application may be running.

For details on how to check the status of the linked cloud service, see [9.5.3 Troubleshooting failures of service linkage jobs and linked cloud services](#).

Note

In the case that multiple executions are not permitted with the linked cloud service and the command defined in the service linkage execution definitions activated, if you re-execute a service linkage job that has been forcibly terminated or reached the termination time, the job may not be executed immediately or an error may occur.

Stop the linked cloud service or the command before re-executing the service linkage job.

5.2.5 Return codes of service linkage jobs

The following table shows return codes when service linkage jobs are executed.

Table 5–2: Return codes of service linkage jobs

Return codes	Content	Corresponding messages
0	Ended normally	--
1 to 50	This is the return code set according to the definitions, if any, on the JP1/AJS3 for Cloud Service Applications server.	KNBB6301-E KNBB6302-E KNBB6303-E
60	Failed to obtain an environment variable.	KNBB6400-E
61	Contains an error in the environment variable or the definition items of the JP1/AJS3 for Cloud Service Applications server.	KNBB6100-E
62	Failed to read the environment setting parameter.	KNBB6401-E
63	Contains an error in the environment setting parameter.	KNBB6101-E
70	Failed to read the connection configuration file.	KNBB6200-E
71	Contains an error in the connection configuration file.	KNBB6201-E
80	Failed to resolve the name (IP address resolution) of the JP1/AJS3 for Cloud Service Applications server.	KNBB6204-E
81	Failed to connect to the JP1/AJS3 for Cloud Service Applications server.	KNBB6202-E
82	An error occurred in communication with the JP1/AJS3 for Cloud Service Applications server.	KNBB6203-E
83	Contains an error in the information obtained from the JP1/AJS3 for Cloud Service Applications server.	KNBB6300-E
90	Failed to execute the command from the service linkage job.	KNBB6304-E
100	A memory shortage occurred.	KNBB6450-E
110	System error.	KNBB6451-E
120	An unexpected error occurred.	KNBB6452-E
Signal no.+128	The command executed by the service linkage job has received a signal and ended.	KNBB6305-E

5.3 Notes on execution of service linkage jobs

- A service linkage job obtains the latest information on the JP1/AJS3 for Cloud Service Applications server. Therefore, if you change definitions used for the service linkage jobs on the JP1/AJS3 for Cloud Service Applications server, the service linkage job may not correctly operate.
When changing definitions on the JP1/AJS3 for Cloud Service Applications server, make sure that the service linkage job operates correctly.
- Service linkage jobs are custom jobs. As with existing custom jobs, the return codes that can be checked with JP1/AJS3 include the return codes of service linkage jobs and the return codes set by JP1/AJS3, which is described in 7.10.3 *Checking the return code of a job* in the *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*.
- Check in advance if a command can be executed in the environment before executing a service linkage job. When the command defined on the JP1/AJS3 for Cloud Service Applications server does not exist, the command defined on the JP1/AJS3 for Cloud Service Applications server ends with a return value other than 0.
- Make sure that the sizes of the standard output and standard error output of the command defined on the JP1/AJS3 for Cloud Service Applications server are not too large. We recommend that the total size of standard output and standard error output is approximately 3 MB (megabyte).
If the size is large, the service linkage job behaves as follows:
For Windows:
The service linkage job ends with a return value of "100" (insufficient memory).
For Linux:
The process of the service linkage job is stopped by the kernel, the status of the service linkage job is "Forcibly terminated", and the return value is "-1".
- Make sure that the full unit name[#] of the service linkage job does not contain the following characters (some of the symbols and characters that can be used for migration from the previous product (JP1/AJS)).
" \
If the full unit name[#] contains any of the above characteristics, the service linkage job ends with a return value of "82".

Contains the job net name and job group name in the upper layer of the job
- When the execution host of the service linkage job is on Windows, there is a limitation on the number of characters of OS command lines. Set the number of characters of command lines (command lines after the variable replacement) defined on the JP1/AJS3 for Cloud Service Applications server to be approximately 8000. If the number of characters exceeds the limitation on OS command lines, the command defined on the JP1/AJS3 for Cloud Service Applications server ends with a value other than 0.

6

Management operation of service linkage monitoring jobs

This chapter describes the procedure for executing a service linkage monitoring job defined on JP1/AJS3 for Cloud Service Applications in JP1/AJS3.

6.1 Types and execution of service linkage monitoring jobs

You can execute service linkage monitoring jobs as monitoring jobs after creating their monitoring definitions for monitored cloud services.

Each monitoring job is executed using the information defined on the JP1/AJS3 for Cloud Service Applications server and the definition information of the custom event job definition executed on JP1/AJS3 - Manager. The service linkage monitoring information for each monitoring job is obtained from the JP1/AJS3 for Cloud Service Applications server where its definition resides and varies depending on the type of the job.

For a list of monitoring information acquired by service linkage monitoring jobs, see [1.1.2\(2\) Function to define service linkage monitoring job information](#).

As described above, a service linkage monitoring job is executed in the order shown below based on the definition on the JP1/AJS3 for Cloud Service Applications server.

Connection definitions (Connection processing)

When connection processing is defined in the connection definitions, the processing for connecting to the cloud service runs in accordance with the information defined in **Execution command settings**, **Execution result judgment (monitoring definition)**, and **Trace information settings (monitoring definition)**.

When the connection processing result is *normal*, the processing is executed according to the object monitoring definitions.

Monitoring definitions (Monitoring processing: Execution command settings)

In monitoring processing, the following processing is executed according to the execution command settings:

- Execute the execution command (information acquisition command).
- Extract the obtained results according to the JMESPath query syntax to store them in the storage destination of the monitored items.

Connection definitions (Connection termination processing)

When connection termination processing is defined in the connection definitions, the processing for termination for the cloud service runs in accordance with the information defined in **Execution command settings**, **Execution result judgment (monitoring definition)**, and **Trace information settings (monitoring definition)**. Note that this processing is not executed if the connection processing has failed with an error.

Monitoring definitions (Monitoring processing: Execution result judgment)

1. In monitoring processing, the processing of determining whether the monitoring condition is met is executed based on the execution result judgment.
2. The following processing is executed after the time period specified for the monitoring interval elapses:
 - Compare the current value of the monitored item stored in **Monitoring processing: Execution command settings** with the previous value according to the monitoring condition configured in the custom event job definition.
 - If the monitoring condition is found to be met after the comparison, put the value in the passing information and end the job normally.
 - If the monitoring condition is found not to be met after the comparison, continue the monitoring.

Note that if the return code of the executed command is *abnormal*, different processing is executed: the job ends abnormally or monitoring is continued according to your setting.

If **Monitoring continues** is selected in the above monitoring processing, the period specified for the monitoring interval elapses, the authentication definition is read, the connection processing described in Connection definitions (Connection processing), Monitoring definitions (Monitoring processing: Execution command

settings), and Monitoring definitions (Monitoring processing: Execution command settings) is executed again, and then the monitoring processing described in this section is executed.

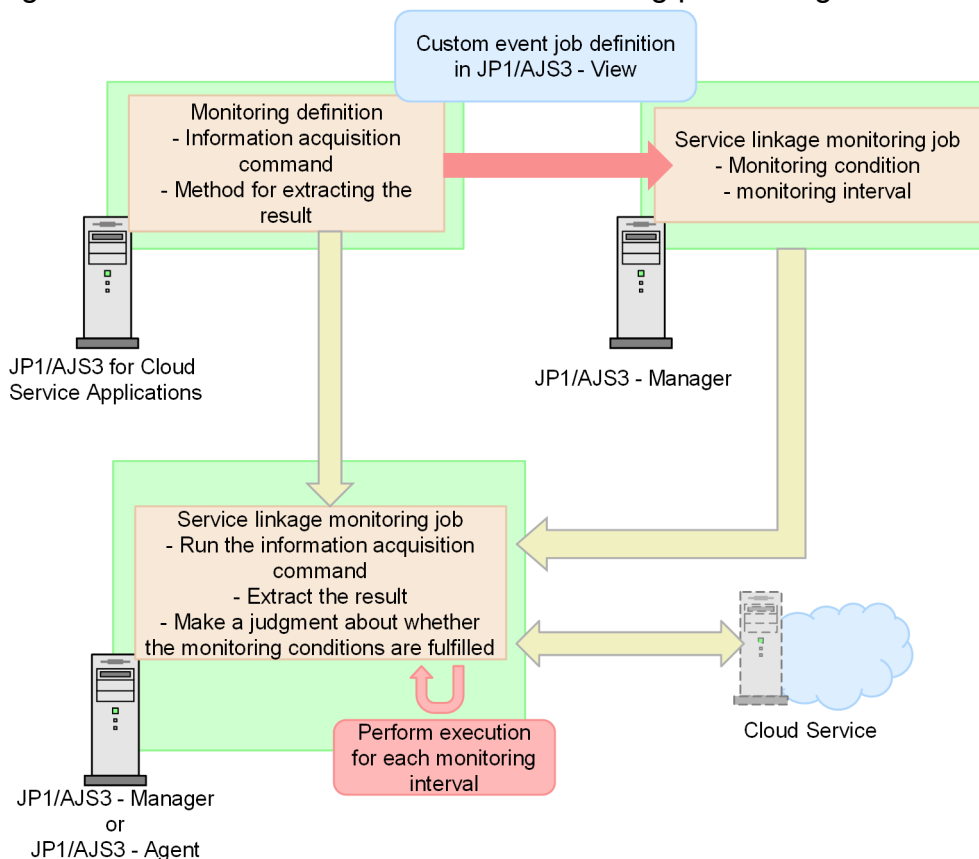
Monitoring definitions (Passing information settings)

If the passing information settings are defined in the monitoring definition, the values are set for the passing information name of the custom event job according to the definition when the monitoring job ends normally. However, they are not set if the job ends abnormally.

The above descriptions of the execution processing are independent of the type of service linkage monitoring jobs.

The figure below explains the general flow of execution of the monitoring processing.

Figure 6–1: Flow of execution of the monitoring processing



For detailed specifications of, for example, the processing for making a judgment about whether the monitoring condition for each of the types shown above is established, see [6.2 Details of service linkage objects monitoring jobs](#).

6.2 Details of service linkage objects monitoring jobs

This section describes the details of service linkage objects monitoring jobs.

6.2.1 Monitoring functions of service linkage objects monitoring jobs

The monitoring function provided by the service linkage object monitoring job is a function that detects objects created, deleted, or updated on an object storage service in a cloud environment. Here, detailed information about the function and processing related to the monitoring processing for detecting this event is presented.

(1) About the details of events to be monitored and the monitoring processing

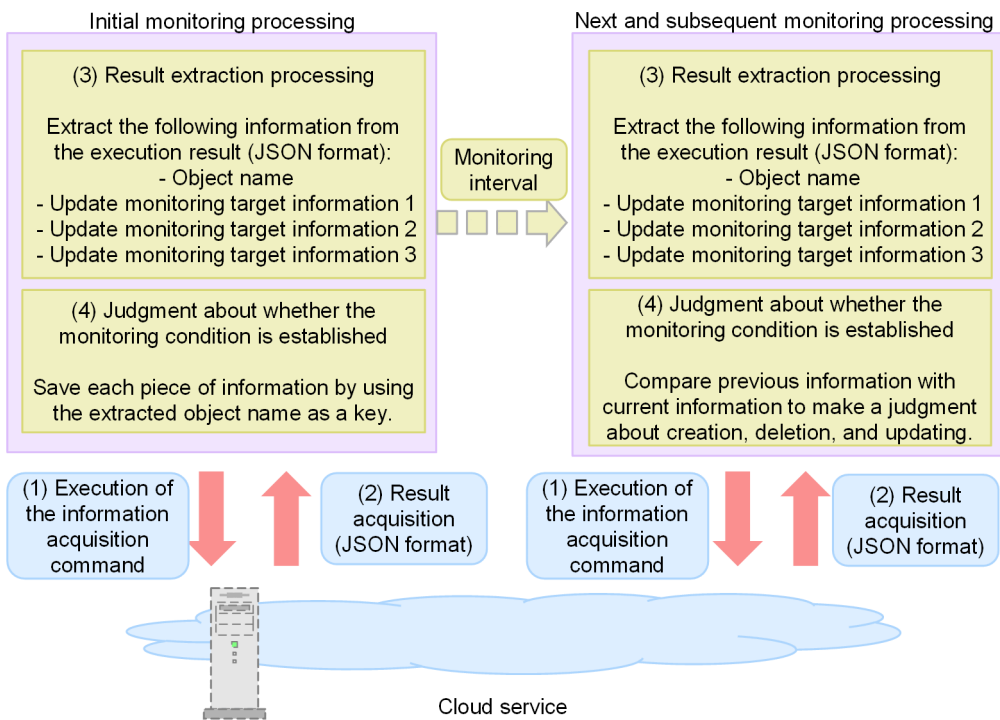
The following explains the events monitored by cloud service linkage object monitoring jobs:

Table 6–1: Types and details of events to be monitored

Item	Event type	Description of operations and conditions for detection
1	Creation	If an object that did not exist at some point in time does exist during the next monitoring interval, JP1 determines that the object has been created and issues an event notification. In addition, if an object already exists when the monitoring is performed for the first time, you can select an option for whether that established that the condition is met.
2	Deletion	If an object that did exist at some point in time does not exist during the next monitoring interval, JP1 determines that the object is deleted and issues an event notification. In addition, if the object does not exist when the monitoring is performed for the first time, you can select an option for whether that establishes that the condition is met.
3	Update	If an object existed at some point in time and a change occurs to an information value of the object during the next monitoring interval, JP1 determines that the object is updated and issues an event notification. Up to three information items can be specified as the monitoring targets. If multiple items are specified, the OR condition is used to determine whether the condition is established.

Details of the event detection processing described above are shown below.

Figure 6–2: Details of the event detection processing



As explained above, extracted information is saved when the monitoring is performed for the first time. During the subsequent monitoring processes, JP1 compares the extracted information with the previously monitored information and determines whether the monitoring conditions for creation, deletion, and update are established.

JP1 uses the following criteria to determine whether the conditions are established:

For creation

It is considered that creation is performed if the object name specified as the monitoring target object name matches one of the extracted object names that did not exist previously. If the initial monitoring option is specified, the condition is met if a matching object exists when the monitoring starts.

For deletion

It is considered that deletion is performed if the object name specified as the monitoring target object name matches one of the extracted object names that existed previously. If the initial monitoring option is specified, the condition is met if no matching object exists when the monitoring starts.

For update

If the object name specified as the monitoring target matches the object name of the objects with differences in the extracted update monitoring target information compared to the previous monitoring, it is considered updated.

For details on behavior when the information acquisition command runs, see [6.2.1\(2\) Behavior when the information acquisition command runs](#). For details on the extraction processing, see [6.2.1\(3\) Processing for extracting object information on the cloud service](#). For details on how to specify the monitoring target object name, see [6.2.1\(4\) About how to specify the names of monitoring target objects](#).

(2) Behavior when the information acquisition command runs

There is an upper limit to the size that can be handled, because memory resources are consumed by the standard output and the standard error output for the information acquisition command to be executed for the monitoring processing.

When over the upper limit of the standard output, output the KNBB6306-E message to the service linkage object monitoring job log file, and the service linkage object monitoring job is terminated with abnormal.

You can change the upper limit value of the standard output with the environment setting parameter `LimitObjMonStdOutSize`.

The upper limit on the standard error output is 3,072 KB.

When over the upper limit of the standard error output, output the KNBB6307-W message to the service linkage object monitoring job log file, and the service linkage object monitoring job continues.

For each, consider using command options in a way that the amount of information to be acquired by the information acquisition command during operation will not exceed the upper limit explained above.

(3) Processing for extracting object information on the cloud service

A service linkage objects monitoring job executes a command to acquire object list information, extracts object names and updates monitoring target information from the list information, and determines whether the monitoring condition is met. It can have up to three update monitoring targets.

The service linkage objects monitoring job can deal with the object list information in JSON format. The object names and update monitoring target information are extracted by analyzing the JMESPath query syntax.

The results extracted through the JMESPath query syntax analysis must meet the following conditions:

- The extraction result of an object name must be a JSON array with a string as its element^{#1, #2}.
- The extraction result of update monitoring target information^{#3, #4} must be a JSON array with one of strings, numeric values^{#5}, or Boolean values and null values as its element (mix of types allowed).
- If update monitoring target information^{#3, #4} is specified, the number of values to be extracted must be equal to the number of array elements of **Object name**^{#6}.

#1

If the same object name is output several times within an array, the update information of the last output number of array elements is enabled.

#2

Null characters cannot be used for object names.

#3

The update monitoring target information is an optional item and therefore does not need to be specified if update monitoring is not enabled in the monitoring condition. In addition, if you want to enable update monitoring, specify up to three monitoring targets.

#4

If nothing is specified for the update monitoring target information even though update monitoring is enabled in the monitoring condition, a KNBB6103-E message is output to the service linkage objects monitoring job log file and the service linkage objects monitoring job ends abnormally.

#5

Numeric data must be an integer value with a range from -10,995,116,277,760 to 10,995,116,277,760. Values other than this value (values outside the scope, decimal fractions, and exponent notations) are rounded to other values and might not be extracted to valid values. Therefore, the processing for monitoring completion might not work properly. Alternatively, the object monitoring job might be terminated abnormally with the KNBB6107-E message saying that numerical information that cannot be handled by service linkage object monitoring jobs was detected.

The update monitoring targets do not have to be specified in the same order of the definitions of **Update monitoring target 1**, **Update monitoring target 2**, and **Update monitoring target 3**. Check that the number of update information fields with a value specified for it is the same as the number of object name elements.

A KNBB6106-E message if the above conditions are not met, or a KNBB6105-E message if an error occurs in extract processing according to the JMESPath query syntax is output to the service linkage objects monitoring job log file. Then the service linkage objects monitoring job ends abnormally.

Verify that the above specifications work for extraction and then configure monitoring processing. For the JMESPath query syntax, see the JMESPath official website.

As shown in the following example, you can extract a list of object names and the size, the update date/time, and the owner of each object from the standard output result of the information acquisition command as the update monitoring target information and use this information as the monitoring target:

- Information acquisition command (displays a list of objects below `/objects` in JSON format)

```
get-object-info list /objects
```

- Command execution result (Object names, update dates/times, sizes, and owners are displayed as object list information in the standard output)

```
{
  "Information": [
    {
      "ObjectName": "object01",
      "ObjectUpdateTime": "2024-09-01T00:00:00+00:00",
      "ObjectSize": 100,
      "ObjectOwner": "User01"
    },
    {
      "ObjectName": "object02",
      "ObjectUpdateTime": "2024-09-01T12:30:30+00:00",
      "ObjectSize": 200,
      "ObjectOwner": "User02"
    }
  ]
}
```

- Specification methods and extraction results related to the extraction processing (JMESPath query statement)

```
Object name
  Specification method: Information[].ObjectName
  Extraction result: [ "object01", "object02" ]
Update monitoring target 1 (update date/time)
  Specification method: Information[].ObjectUpdateTime
  Extraction result: [ "2024-09-01T00:00:00+00:00", "2024-09-01T12:30:30+00:00" ]
Update monitoring target 2 (size)
  Specification method: Information[].ObjectSize
  Extraction result: [ 100, 200 ]
Update monitoring target 3 (owner)
  Specification method: Information[].ObjectOwner
  Extraction result: [ "User01", "User02" ]
```

The extracted information (see above) and the specifications in 6.2.1(4) *About how to specify the names of monitoring target objects* are used to carry out the monitoring processing as shown in 6.2.1(1) *About the details of events to be monitored and the monitoring processing*.

(4) About how to specify the names of monitoring target objects

The name of an object to be monitored is specified in the custom event job definition.

You can specify a monitoring object with a single object name or monitoring objects with multiple object names. You need to specify a generic name with a wildcard character (*) to specify multiple objects. A generic name can use the wildcard character (*) only.

Review the following notes if you use the wildcard:

- The * section matches any character string.
- If you want to use the asterisk (*) itself, use a preceding \ character to escape the asterisk (*).
- If you want to use the backslash (\) itself, use a preceding \ character to escape the backslash (\).
- If a character other than the asterisk (*) is specified immediately after a backslash (\), the backslash (\) is ignored.
Example: If \a is specified, it is handled as a.
- If a character string ends with a backslash (\), the backslash (\) is ignored.
Example: If a\ is specified, it is handled as a.
- If two or more consecutive asterisks (*) are specified, the second and subsequent asterisks (*) are ignored.
Example: If a** is specified, it is handled as a*.

6.2.2 Service linkage objects monitoring job execution environment and permissions

This subsection describes the execution environment, such as the process structure, and access permissions to resources when service linkage objects monitoring jobs are executed.

(1) Process structure for service linkage objects monitoring

A service linkage objects monitoring daemon must be started on the monitoring job execution host to use service linkage objects monitoring jobs.

The following figure and table show the OS user who executes service linkage objects monitoring jobs and information acquisition commands, and the process structure.

Figure 6–3: OS user when executing service linkage objects monitoring jobs

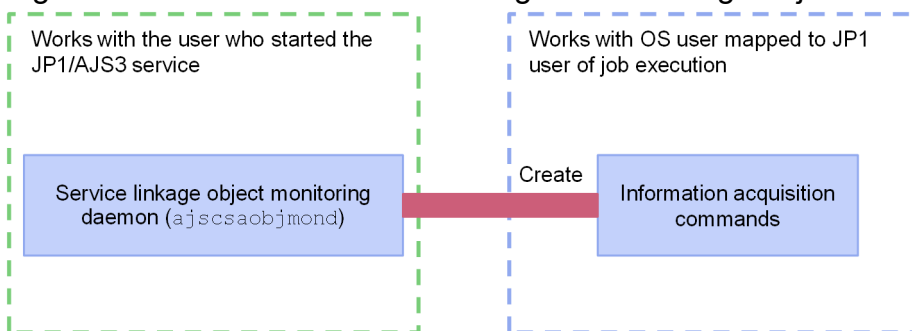


Table 6–2: Parent-child relationship of execution processes

Process name (number of processes)		Description
jajs_spmd (1)		JP1/AJS3 service
jpoagent (1)		Event/action control agent process
jpoagtsub (1)		Event/action control subagent process
ajscsaobjmond (1)		Service linkage objects monitoring daemon. It is a resident process that controls execution of monitoring processing of service linkage objects monitoring jobs.
Information acquisition command (1 or more)		Is started when monitoring processing is executed (at monitoring intervals). When multiple jobs are executed concurrently, the number of processes increase based on the number of concurrently executed jobs.

The service linkage objects monitoring daemon above is a process that is started when you start the JP1/AJS3 service with the `CloudObjectMon` environment setting parameter specified. For the function to start the JP1/AJS3 service, see the JP1/AJS3 manual.

(2) Execution permissions of service linkage objects monitoring jobs

As described in (1), a service linkage objects monitoring job is started by the service linkage objects monitoring daemon. Therefore, files such as log files and connection configuration files are operated with the permissions of the user who started the JP1/AJS3 service.

Furthermore, the following is executed based on the JP1 user defined by the **Executed by** value specified for the custom event job:

- Information acquisition command by a mapped OS user
- Communication with the JP1/AJS3 for Cloud Service Applications server

With the permissions for operation previously mentioned in mind, consider the appropriate user who starts the JP1/AJS3 service, JP1 user, and mapped OS user.

(3) Environment variables when information acquisition commands are executed

Environment variables are set by service linkage objects monitoring jobs when commands are executed. These variables take effect in the following order of priority (with the highest priority of 1).

- In Windows
 1. Environment variables specified separately by a command
 2. Environment variables specified as global
 3. Environment variables for the job execution user
 4. Environment variables specified when the service is started
- In Linux
 1. Definitions in the local login script
 2. Definitions in the system login script
 3. Environment variables set separately by a job[#]

4. Environment variables specified separately by a command
5. Environment variables specified as global
6. Environment variables specified when the service linkage object monitoring daemon is started

#

The following table lists the environment variables to be set.

Table 6–3: Environment variables set separately by a job

No.	Environment variable name	Value to be set
1	HOME	Login directory defined in the password file of the command execution user
2	SHELL	Login shell defined in the password file of the command execution user

(4) Where the current directory is when information acquisition commands are executed

The current directory when a command is executed is the *service linkage objects monitoring job temporary file folder (directory)*. For the exact path, see *A. Files and Directories*.

All the files under the service linkage objects monitoring job temporary file folder (directory) are deleted when the service linkage objects monitoring daemon is started. Avoid an operation in which command execution results in saving any files in the current directory.

(5) When and what information do service linkage objects monitoring jobs read

A service linkage objects monitoring job reads the following information using the permissions in (2):

- Connection configuration file used to access JP1/AJS3 for Cloud Service Applications
- Definition information below, defined in the JP1/AJS3 for Cloud Service Applications server:
 - Connection definition information
 - Authentication definition information
 - Service linkage objects monitoring definition information

The above information, except for the authentication definition information, is read by the service linkage objects monitoring job when started. The authentication definition information is read both when the job is started and at monitoring intervals.

As mentioned above, you do not have to stop the job when you want to update the authentication information. You will have access to the cloud service by updating it while the job is running.

6.2.3 Behavior when the JP1/AJS3 service is started and stopped

This subsection describes the job statuses of service linkage objects monitoring jobs.

(1) Statuses when the service is started or stopped

The service is started or stopped according to the JP1/AJS3 specifications. The status at this time is determined by the specifications of custom event jobs. See the specifications of custom event jobs in the manual *JP1/Automatic Job Management System 3 Administration Guide*.

However, for in what status the service linkage objects monitoring job in *Running* status before the service is stopped will be started, see (2).

(2) How the service linkage objects monitoring job works after the service is restarted

The following describes the operation that occurs after the service stops while a service linkage objects monitoring job is running and then the service is restarted with *hot start*.

(a) How the monitoring status can be passed after the service is restarted

When a service linkage objects monitoring job enters the *Running* status, the data can be stored in files whenever necessary while monitoring objects are monitored. In this way, even if the JP1/AJS3 service stops, the previous monitoring status can be restored after its restart.

Note that no events can be detected if they occur between the service stop and the resumed event monitoring after the service restart. If the file into which the data is stored cannot be opened, a KNBB6162-W message is output to the process log of the execution agent and the integrated trace log. Also, if the file has an invalid format, a KNBB6403-W message is output to the service linkage file monitoring job log and the integrated trace log. In both cases, monitoring continues.

(b) Definition after the service is restarted

If you modify the definition[#] of a service linkage objects monitoring job while monitoring is continued after the service is restarted, when you restart the JP1/AJS3 service, the job works with the definition at the recent execution registration unless the execution registration is performed again.

#

The *definition* refers to a definition on the custom event job. For a service linkage objects monitoring job, the definitions of *Monitoring objects*, *Monitoring interval*, and *Monitoring options* in JP1/AJS3 for Cloud Service Applications use the ones read when the job goes running after the JP1/AJS3 - Agent service is started, regardless of a change of the job definition in JP1/AJS. For details about the operation that occurs after JP1/AJS3 for Cloud Service Applications definitions are changed, see (c) *JP1/AJS3 for Cloud Service Applications definitions after the service is restarted*.

(c) JP1/AJS3 for Cloud Service Applications definitions after the service is restarted

When a definition in JP1/AJS3 for Cloud Service Applications is modified, the job also works with the definition read when the job goes running after the JP1/AJS3 service is started, as described in (b) *Definition after the service is restarted*.

6.2.4 Passing information of service linkage objects monitoring jobs

This subsection describes passing information of service linkage objects monitoring jobs.

(1) Passing information of service linkage objects monitoring jobs

In JP1/AJS3 for Cloud Service Applications, you can define what values are stored in which variables so that the values can be passed to succeeding jobs.

These variables are used to define information to be passed on for OBJECT01 through OBJECT10, which are names of passing information for the custom event job.

For example, following shows the definition example when a format, used to access a target object, which is created by combining both a packet name and an object path, *//packet-name/object-path*, is passed.

You use a variable, `?CSAONAME?`, obtained as an object name through the JMESPath query syntax from the execution result of the information acquisition command for the object.

For example, assume that an object with the name `20230915_s1_report1.txt` is detected in the path with the name `/ABC/DEF/` to objects under the bucket with the name `mybucket`. To specify `//mybucket/ABC/DEF/20230915_s1_report1.txt` for the passing information name OBJECT01, in **Passing information settings** of the service linkage objects monitoring definition, enter `//mybucket/ABC/DEF/?CSAONAME?` in **OBJECT01** under **Name of passing information to be used as the storage destination**.

In JP1/AJS3 - View, enter `?AJS2URI?:OBJECT01` in **Passing** of the unit definition for the service linkage objects monitoring job. This allows succeeding jobs to receive the information of the format used to access the target object using `?AJS2URI?`.

The following explains the details of the variables to be used for OBJECT01 through OBJECT10, which are names of passing information for the custom event job.

(a) Values to be saved in the variables

Values set as passing information are determined by the data types of extraction position information. The following table shows the details.

Table 6–4: Information to be saved in the variables

No.	Data type	Information to be saved in the variables
1	Character string	The character string value is set as it is.
2	Number	Specify a numerical value that is presented as a character string and can be handled as a product.
3	Boolean	true or false is set.
4	Null	null is set.

(b) About the variables in which object names will be saved

The information extracted by the JMESPath query statement specified in the object name is saved in the variable `?CSAONAME?`.

The name of the created, updated, or deleted object is saved when creation, update, or deletion is monitored. However, when deletion is monitored and detected, a null string is saved in the variable if the condition is to be established when no objects exist.

(c) About the variables in update monitoring target information

Information extracted by the JMESPath query statement specified in the three pieces of update monitoring target information is saved in the variables ?CSAOINFO1?, ?CSAOINFO2?, and ?CSAOINFO3?. However, if the JMSPPath query statement is omitted in the monitoring definition, no values are set in the omitted update monitoring target information variables after the monitoring is completed.

In addition, after the monitoring for creation, update, and deletion is completed, the following values are set:

- In the case of creation
A value extracted by the JMESPath query statement specified in individual pieces of update monitoring target information in the object of which creation can be detected.
- In the case of an update
A value extracted by the JMESPath query statement specified in individual pieces of update monitoring target information in the object to which updates can be detected.
- In the case of deletion
A value extracted by the JMESPath query statement specified in individual pieces of update monitoring target information acquired during the previous monitoring.
As in the case of an object name, when deletion is detected, a null character is set if the condition is to be established when there are no objects.

(d) About system-reserved variables that can be used by default

Service linkage object monitoring jobs have the following variables, in addition to the system-reserved variables that can be used by default and are explained in [4.3.2\(1\) Types of variables](#):

Variable name	Description
?CSASOBJCOND?	Upon completion of monitoring, save one of the following monitoring conditions that have been met: <ul style="list-style-type: none">• c (creation)• d (deletion)• u (update)

6.2.5 Execution results of service linkage objects monitoring jobs

You can see if the monitoring condition is met for a service linkage objects monitoring job and what error occurred in the Execution result details dialog box of JP1/AJS -View or JP1/AJS3 - Web Console using **Output settings for detailed execution results** on the monitoring definition. For details about the Execution result details dialog box of JP1/AJS -View or JP1/AJS3 - Web Console, see the description about the Execution result details dialog box in the manual *JP1/Automatic Job Management System 3 Operator's Guide*.

6.2.6 Forced termination of service linkage objects monitoring jobs

The following table shows the operation when a service linkage objects monitoring job is forcibly terminated (killed) and when the timeout time is reached.

Table 6–5: Operation when a service linkage objects monitoring job is forcibly terminated

Target		Status
Manager	Job on the scheduler service	The status of the service linkage objects monitoring job turns to <i>kill</i> .
Execution destination (Agent)	Information acquisition command (if it is running)	The information acquisition command is still running.

6.2.7 Return codes of service linkage objects monitoring jobs

The following table shows return codes when service linkage objects monitoring jobs are executed.

Table 6–6: Return codes of service linkage objects monitoring jobs

Return code	Content	Corresponding messages
0	The monitoring condition is met.	--
101 to 150	This is the return code set according to the definitions, if any, on the JP1/AJS3 for Cloud Service Applications server.	KNBB6310-E
151	The definition of the service linkage objects monitoring job contains an error.	KNBB6102-E
152	<ul style="list-style-type: none"> In the agent host, the manager host name specified as the server host name for the JP1 user is incorrect. In the user mapping definition of the agent host, the applicable JP1 user is not registered. In the user mapping definition of the agent host, an OS user that does not exist is registered. In the user mapping definition of the agent host, an incorrect OS user password is registered (Windows only). A JP1 user with the same name as that of the OS user who executed the <code>ajsentry</code> command is not found. The owner JP1 user is different from the JP1 user who performed the execution registration. There is an ongoing memory shortage. When Owner user is specified in Executed by and Owner is empty in the detailed definition of the job, the name of the OS user who is not registered as a JP1 user is set for the startup account of the JP1/AJS3 service on the manager host. 	KNBB6309-E
153	Failed to read the connection configuration file.	KNBB6200-E
154	The syntax in the connection configuration file has an error.	KNBB6201-E
155	Failed to resolve the name (IP address resolution) of the JP1/AJS3 for Cloud Service Applications server.	KNBB6204-E
156	An error occurred during access to the temporary file.	KNBB6449-E
170	Failed to connect to the JP1/AJS3 for Cloud Service Applications server.	KNBB6202-E
171	An error occurred in communication with the JP1/AJS3 for Cloud Service Applications server.	KNBB6203-E
172	The information obtained from the JP1/AJS3 for Cloud Service Applications server contains an error.	KNBB6300-E
173	<p>A definition item for JP1/AJS3 for Cloud Service Applications has one of the following errors:</p> <ul style="list-style-type: none"> The mandatory item is left blank. 	KNBB6100-E

Return code	Content	Corresponding messages
173	<ul style="list-style-type: none"> Number of characters Format of the value 	KNBB6100-E
175	<p>A definition of the service linkage objects monitoring job is inconsistent with the one on the JP1/AJS3 for Cloud Service Applications server.</p> <ul style="list-style-type: none"> Although the Update option is selected in the Monitoring options in the definition of the service linkage objects monitoring job, any update monitoring target is not specified in the definition on the JP1/AJS3 for Cloud Service Applications server. 	KNBB6103-E
176	An error occurred in the extraction processing of information from the execution result of the object list information acquisition command according to the JMESPath query syntax.	KNBB6105-E
177	The result extracted from the object list information is incorrect.	KNBB6106-E
178	The update monitoring target data extracted from the object list information is in valid format.	KNBB6107-E
180	Failed to obtain an environment variable.	KNBB6400-E
181	An error occurred in the command executed by the service linkage objects monitoring job.	KNBB6311-E
182	The command executed by the service linkage objects monitoring job has received a signal and ended.	KNBB6312-E
183	The size of the standard output for the command executed by the service linkage objects monitoring job exceeded the value of the <code>LimitObjMonStdOutSize</code> environment setting parameter.	KNBB6306-E
190	A memory shortage occurred.	KNBB6450-E
191	System error.	KNBB6451-E
192	An unexpected error occurred.	KNBB6452-E

Note

If you work with the entire start condition (when the start condition is forcibly terminated, for example) or if an error related to the entire start condition occurs, the return code of each event of the entire start condition is set to 0 (zero). On the other hand, if an error on a particular event occurs (when an error occurs due to an incorrect definition, for example), the return code shown in the table is set.

6.2.8 Notes on execution of service linkage objects monitoring jobs

This subsection provides notes on executing service linkage objects monitoring jobs.

- Consider the options of the information acquisition command line executed by service linkage objects monitoring jobs so that the number of objects to be obtained is 5,000 or less. In addition, adjust the configuration of the linked cloud service or the command line of the information acquisition command so that the names of the objects to be obtained each have 128 bytes or less in size. For example, if you run a command with no option specified, trying to obtain the information of all the objects on the cloud service, a command with potential unlimited results can lead to degraded performance of processing, insufficient memory, or the upper limit of the standard output size, resulting in abnormal termination.
- Update the definition for authentication information quickly. A service linkage objects monitoring job reads the definition for authentication information at monitoring intervals while running. However, monitoring continues in a condition where the connection processing to the cloud service ended abnormally or the connection failed. When jobs are running in particular, do so not to interrupt your operation.

- Execution of the information acquisition command might take time and the monitoring might not be performed at the monitoring interval, depending on the status of communication with the cloud environment or when there are numerous objects on the cloud service, etc.
- If you want to guarantee the order of information on objects to be obtained from a cloud service, see the specifications of the information acquisition command you use and specify the object monitoring definition. When a generic name (wildcard character) is used in **Name of the object to be monitored**, the value stored in the passing information depends on the specifications of the information acquisition command. Therefore, verify in what order the information is passed and then design your use of macro variables in succeeding jobs.
- Wildcard characters available in **Name of the object to be monitored** are * and \ that is used to escape *. Other characters such as ., ^, \$, |, [,], (,), {, }, +, ?, which are used as generic names, are treated as literal characters.
- A service linkage objects monitoring job obtains the latest information on the JP1/AJS3 for Cloud Service Applications server. Therefore, if you change definitions used for the service linkage objects monitoring jobs on the JP1/AJS3 for Cloud Service Applications server, the service linkage objects monitoring job may not correctly operate.

When changing definitions on the JP1/AJS3 for Cloud Service Applications server, make sure that the service linkage objects monitoring job operates correctly.

- Service linkage objects monitoring jobs are custom event jobs. The return codes that can be checked with JP1/AJS3 include the return codes of service linkage objects monitoring jobs and the return codes set by JP1/AJS3, which is described in *Checking the return code of a job* in the manual *JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide*.
- Check in advance if a command can be executed in the environment before executing a service linkage objects monitoring job.

When the command defined on the JP1/AJS3 for Cloud Service Applications server does not exist, the command defined on the JP1/AJS3 for Cloud Service Applications server ends with a return value other than 0.

- When the execution host of the service linkage objects monitoring job is on Windows, there is a limitation on the number of characters of OS command lines. Set the number of characters of command lines (command lines after the variable replacement) defined on the JP1/AJS3 for Cloud Service Applications server to be approximately 8000. If the number of characters exceeds the limitation on OS command lines, the command defined on the JP1/AJS3 for Cloud Service Applications server ends with a value other than 0.
- The upper limit on the output size is 10,240 KB, even if settings are made to output the standard output and the standard error output for execution commands in **Output settings for detailed execution results** and **Log output settings** in the monitoring definition.
- When multiple service linkage object monitoring jobs run same time on one agent, monitoring processes are execute parallel.

The maximum number of items that can be monitored in parallel is 20. During the monitoring process, the number of executions is exclusively occupied, and the monitoring process of the subsequent service linkage object monitoring job is in queue. Therefore, the start of the subsequent monitoring processing might be delayed. If there is a possibility that numerous monitoring processes can run at a certain point in time, consider organizing agents into groups.

7

Operation

This chapter describes GUI operations in JP1/AJS3 for Cloud Service Applications.

7.1 Web GUI

This section describes how to operate the Web GUI.

7.1.1 Web browser settings

When using the Web GUI, check the Web browser settings shown below. For details on how to adjust the settings, see the document for your Web browser.

Pop-up blocking setting

If the pop-up blocking setting of the Web browser is enabled, a dialog box of the Web GUI may be blocked. In the pop-up blocking setting of the Web browser, add the address of the CSA server to the site you want to permit so that the pop-up block can be released.

JavaScript setting

The Web GUI requires the JavaScript (Active Scripting) settings to be enabled on your Web browser. The JavaScript (Active Scripting) settings are enabled by default. If disabled, you cannot log in to JP1/AJS3 for the Cloud Service Applications. Also, if the setting is disabled after login, operations after that will be unavailable.

Web storage setting

The Web GUI requires the Web storage (DOM storage and site data) setting to be enabled on your Web browser. The Web storage (DOM storage and site data) setting is enabled by default.

SSL/TLS setting

To use the communication encryption function, the SSL/TLS setting needs to be enabled on the Web browser. The SSL/TLS setting is enabled by default. If the SSL/TLS setting is disabled, the login screen is not displayed even if you access the CSA server. Also, if the SSL/TLS setting is disabled after login, operations after that will be unavailable.

Cautionary note

While using the Web GUI, do not switch the page being displayed to another page or use **Back** or **Next** on the Web browser.

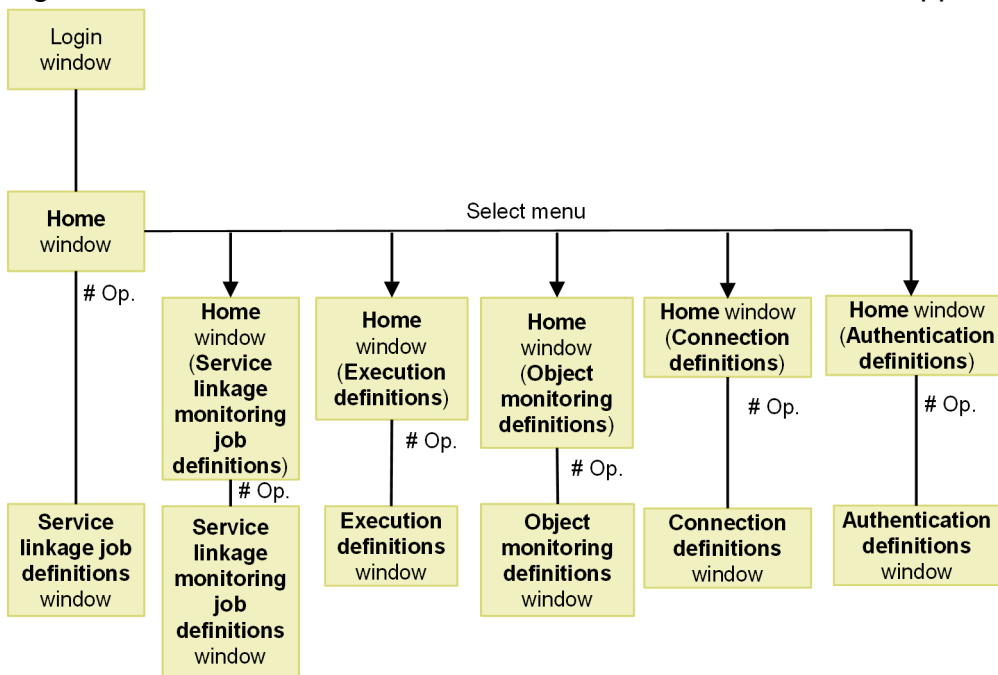
Supplementary note

The language of the Web GUI depends on the setting of your Web browser.

7.1.2 Window transitions

The following figure shows the window transitions in JP1/AJS3 for Cloud Service Applications.

Figure 7–1: Window transitions in JP1/AJS3 for Cloud Service Applications

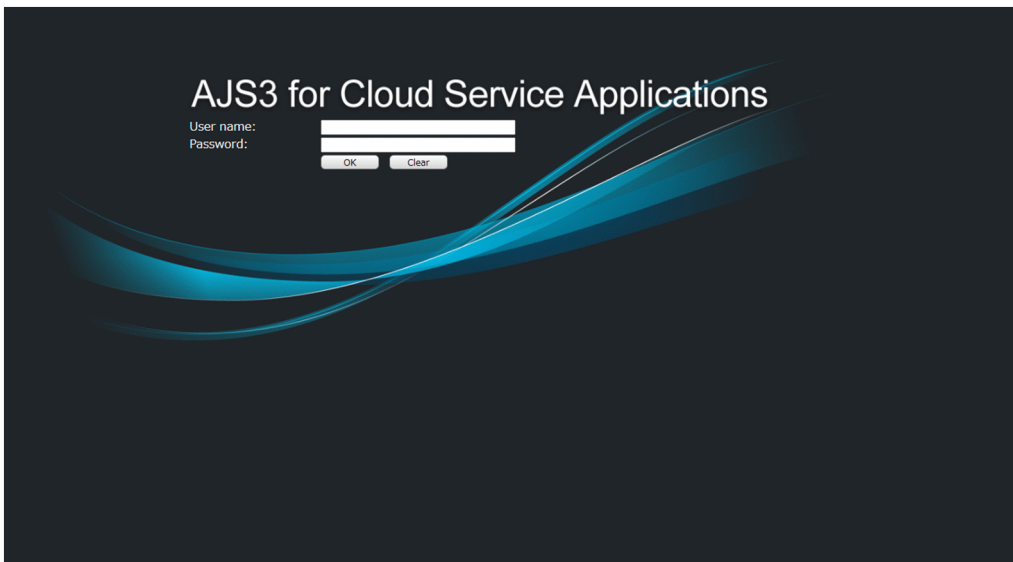


Legend:
 #Op. : Click the Create button or click the definition name in the list

7.1.3 Login window

This section explains about the Login window.

Figure 7–2: Login window



The following shows the display items and input restrictions for the Login window:

User name

Enter the JP1 username to log in.

Password

Enter the password of the JP1 user.

OK button

Enter **User name** and **Password** and click the **OK**.

If there is no problem, the Home window will appear.

Clear button

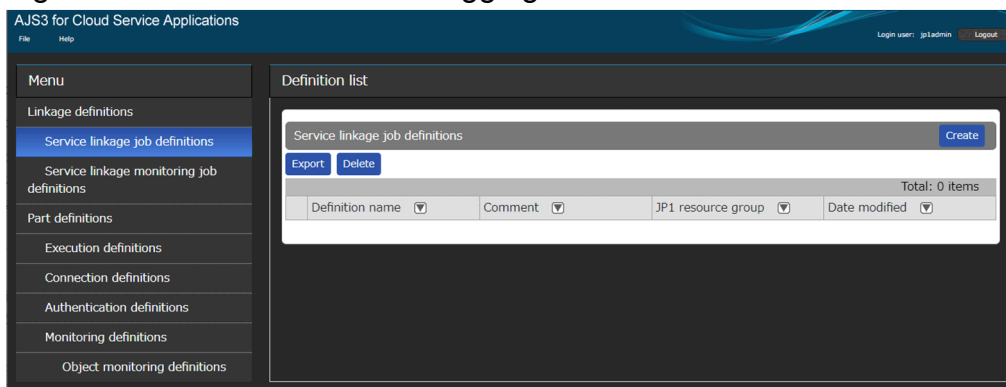
Initialize **User name** and **Password**.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	User name	Text box	Character string of 1 to 31 bytes.	Required	None
2	Password	Text box	Character string of 1 to 32 bytes.	Required	None

7.1.4 Common display items

This section explains display items in common on the top of the screen in each window after logging in to JP1/AJS3 for Cloud Service Applications.

Figure 7–3: The window after logging in



File

Click it to display the following menu items:

Logout

A logout confirmation message is displayed. Click **OK** to return to the login screen.

Help

Click it to display the following menu items:

Version information

Display the **Version information** dialog box.

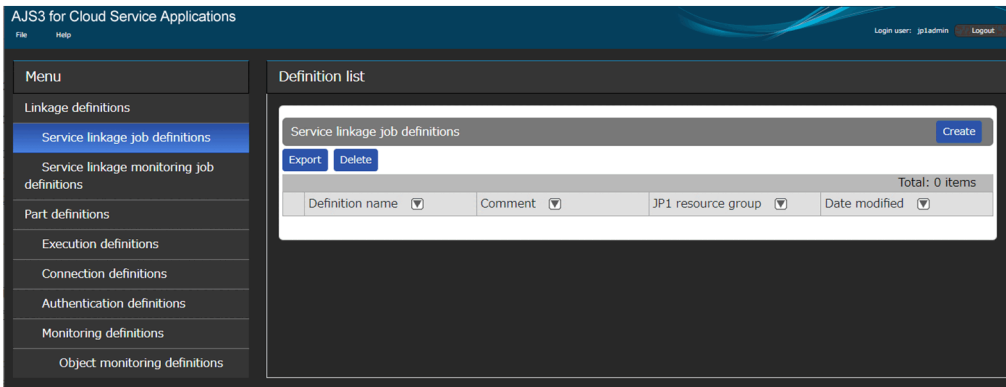
Logout button

A logout confirmation message is displayed. Click **OK** to return to the login screen.

7.1.5 Home window

Home window displays a list of the information defined in the JP1/AJS3 for Cloud Service Applications.

Figure 7–4: Home window



The following shows the display items for the Home window:

Menu

The following items are displayed:

Service linkage job definition

Click this item to display the list of service linkage job definitions registered in the **Definition list**. This item is selected when you log in to the system.

Service linkage monitoring job definitions

Click this item to display the list of service linkage monitoring job definitions registered in the **Definition list**.

Execution definition

Click this item to display the list of execution definitions registered in the **Definition list**.

Connection definition

Click this item to display the list of connection definitions registered in the **Definition list**.

Authentication definition

Click this item to display the list of authentication definitions registered in the **Definition list**.

Monitoring definitions - Object monitoring definitions

Click this item to display the list of object monitoring definitions registered in the **Definition list**.

Definition list

This area lists the definitions of the item you select from the **Menu**. The service linkage job definitions are listed when you log in to the system.

Create button

The screen changes to the new definition screen of the definitions being listed.

Export button

This button outputs the definitions of the items selected in the definition list to a file in JSON format.

Note that this button is not shown while the **Authentication definitions** is displayed.

Delete button

This button deletes the definitions of the items selected in the definition list.

Sort button

When the screen is opened, the data are displayed unsorted. Press (▼) for ascending sorting or (▲) for descending sorting to change the sorting of the definitions. Press the button repeatedly to toggle between ascending and descending order. The data do not return to the unsorted state. Pressing the button in another column changes the column's button to ascending. This action clears sorting from the previously sorted column.

Definition name

This column shows the definition names. Clicking any of the links displays its corresponding definition screen.

Comment

Display the comment of the definition.

JP1 resource group

Display the JP1 resource group of the definition.

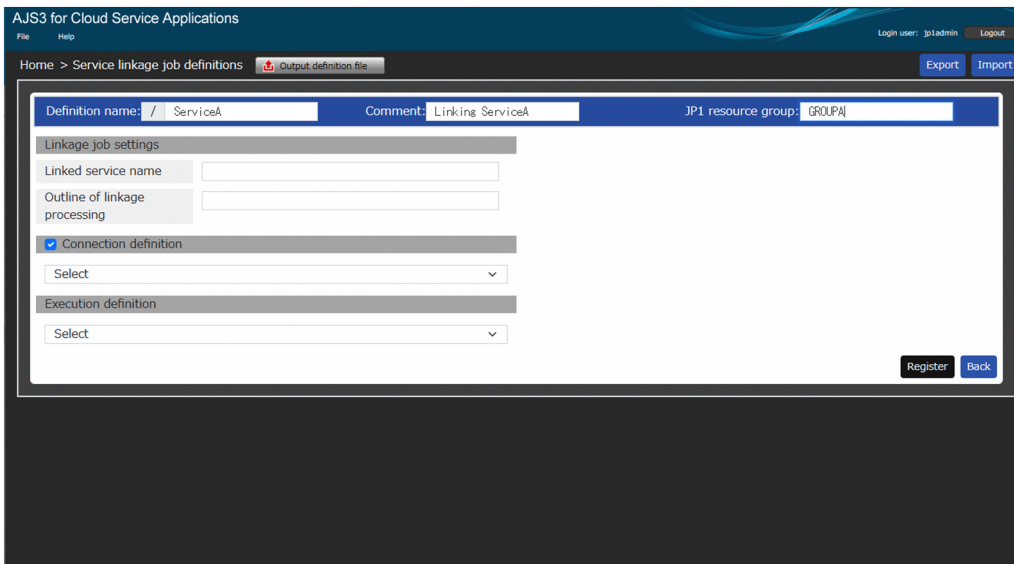
Date modified

The update date and time of the definition is displayed in the format of year, month, date, minutes, and seconds (YYYY/MM/dd HH:mm:ss).

7.1.6 Service linkage job definition window

In the Service linkage job definition window, you can view and edit service linkage job definitions in detail.

Figure 7–5: Service linkage job definition window



The following shows the display items and input restrictions for the Service linkage job definition window:

Definition name

Enter the definition name of the service linkage job information. It is saved in the format of */definition-name*. It cannot be changed when editing.

Comment

Display the comment of the service linkage job information.

JP1 resource group

Display the JP1 resource group of the service linkage job information.

Linkage job settings

Set linkage information of a service linkage job information.

Linked service name

Enter a linkage-destination service name to be linked by the service linkage job. This information can be managed as information that associates the cloud service after job execution. Therefore, complete this item whenever possible.

Outline of linkage processing

Enter the overview of processing to be linked by the service linkage job. This information can be managed as information that associates the executed processing of the cloud service after job execution. Therefore, complete this item whenever possible.

Connection definition

Use this item to show whether or not to use connection definitions for the service linkage job. With this item selected, the drop-down list allows you to select a connection definition. Without this item selected, no drop-down list is displayed.

Execution definition

Select an execution definition to use for the service linkage job from the drop-down list.

Output definition file button

This button displays the Output definition file dialog to output a service linkage job definition information file necessary for registration with JP1/AJS3 -View. For details, see [7.1.6\(1\) Output definition file dialog box](#).

Export button

Clicking this button outputs the service linkage job information being displayed as the service linkage job definitions file (`sljobdefExport.txt`). This file will be output to the download folder set by the Web browser.

For details about a service linkage job definitions file, see [F.3 Service linkage definition file](#).



Note

Even during input of service linkage job definitions, a service linkage job definition file can be exported.

Import button

Click this button to display the Open dialog allowing you to select a service linkage job definition file to be reflected to the screen. Select a service linkage job definition file. It will be reflected on the Service linkage job definitions screen.

For details about the format of a service linkage job definitions file, see [F.3 Service linkage definition file](#).



Note

Even during input of service linkage job definitions, the service linkage job definition file can be imported.

Register button

Click this button to register the service linkage job definitions, which have been input on the Service linkage job definitions screen with JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed. If an error occurs, the item with the error is highlighted.

Back button

Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes.	Not required	JP1_CSA

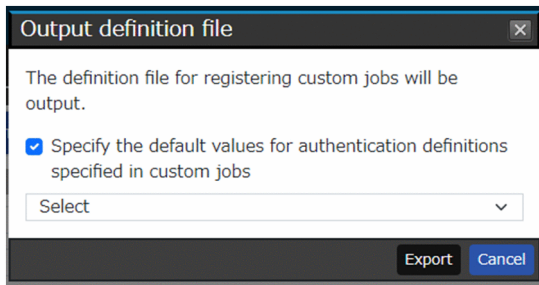
No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
3	JP1 resource group	Text box	Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA
4	Linked service name	Text box	Character string within 150 bytes.	Not required	None
5	Outline of linkage processing	Text box	Character string within 243 bytes.	Not required	None
6	Connection definition	List box	Specify the registered connection definition.	Required [#]	None
7	Execution definition	List box	Specify the registered execution definition.	Required	None

[#]: In case of using a connection definition.

(1) Output definition file dialog box

This section explains about the Output definition file dialog box.

Figure 7–6: Output definition file dialog box



The following shows the display items and input restrictions for the Output definition file dialog box:

Specify the default values for authentication definitions specified in custom jobs

Selecting this item outputs the authentication definition name selected from the pull-down menu as the default value of the authentication definition of the custom job.

Export button

Clicking this button outputs the service linkage job definition information file (`sljobdef.txt`) for registering custom jobs. Do not change the output content of the service linkage job definition information file. Note that depending on the editor software, the character code, line break code, and existence of BOM might change simply by resaving the file.

If the content of the file is invalid, for example, when a BOM is assigned, the KNBB4511-E error occurs when executing the `ajscsajobreg` command for custom job registration, and the processing fails.

Cancel button

Close the dialog box without doing anything.

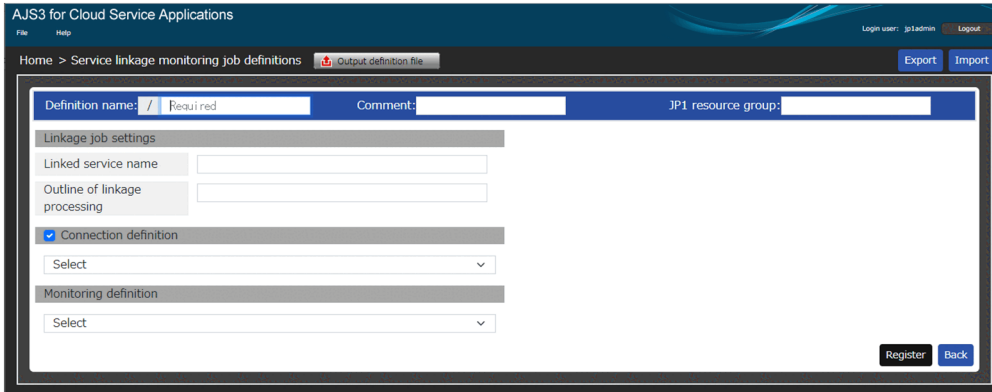
No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Specify the default values for authentication definitions specified in custom jobs	List box	Specify the registered authentication definition.	Required [#]	None

#: In case of specifying a default value of the authentication definition.

7.1.7 Service linkage monitoring job definition window

In the Service linkage monitoring job definition window, you can view and edit service linkage monitoring job definitions in detail.

Figure 7–7: Service linkage monitoring job definition window



The following shows the display items and input restrictions for the Service linkage monitoring job definition window:

Definition name

Enter the definition name of the service linkage monitoring job information. It is saved in the format of / *definition-name*. It cannot be changed when editing.

Comment

Enter the description of service linkage monitoring job information.

JP1 resource group

Enter the JP1 resource group of the service linkage monitoring job information.

Linkage job settings

Set linkage information of the service linkage monitoring job information.

Linked service name

Enter a linkage-destination service name to be linked by the service linkage monitoring job. This information can be managed as information that associates the cloud service after job execution. Therefore, complete this item whenever possible.

Outline of linkage processing

Enter the overview of processing to be linked by the service linkage monitoring job. This information can be managed as information that associates the executed processing of the cloud service after job execution. Therefore, complete this item whenever possible.

Connection definition

Select this to indicate whether or not to use connection definitions for the service linkage monitoring job.

With this item selected, the drop-down list allows you to select a connection definition. The connection definitions displayed are those defined in the JP1/AJS3 for Cloud Service Applications from 13-10.

Without this item selected, no drop-down list is displayed.

Monitoring definition

Select a monitoring definition to use for the service linkage monitoring job from the drop-down list.

Output definition file button

This button displays the Output definition file dialog box to output a service linkage monitoring job definition information file necessary for registration with JP1/AJS3 - View. For details, see [7.1.7\(1\) Output definition file dialog box](#).

Export button

Clicking this button outputs the service linkage monitoring job information being displayed as the service linkage monitoring job definition file (`slmonjobdefExport.txt`). This file will be output to the download folder set by the Web browser.

For details about the service linkage monitoring job definition file, see [G.2 Service linkage monitoring job definition file](#).



Note

Even during input of service linkage monitoring job definitions, a service linkage monitoring job definition file can be exported.

Import button

Click this button to display the Open dialog allowing you to select a service linkage monitoring job definition file to be reflected to the screen. Select a service linkage monitoring job definition file. It will be reflected on the Service linkage monitoring job definition window.

For details about the format of service linkage monitoring job definition files that can be imported, see [G.2 Service linkage monitoring job definition file](#).



Note

Even during input of service linkage monitoring job definitions, the service linkage monitoring job definition file can be imported.

Register button

Click this button to register the service linkage monitoring job definitions, which have been input on the Service linkage monitoring job definition window with JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed.

If an error occurs, the item with the error is highlighted.

Back button

Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes. Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA
4	Linked service name	Text box	Character string within 150 bytes.	Not required	None
5	Outline of linkage processing	Text box	Character string within 243 bytes.	Not required	None

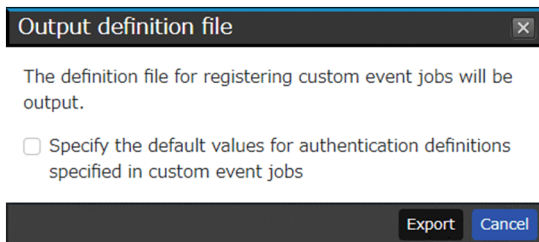
No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
6	Connection definition	Text box	Specify the registered connection definition.	Required [#]	None
7	Monitoring definition	Text box	Specify the registered monitoring definition.	Required	None

[#]: In case of using a connection definition.

(1) Output definition file dialog box

This section describes the Output definition file dialog box launched from the Service linkage monitoring job definition window.

Figure 7–8: Output definition file dialog box in the Service linkage monitoring job definition window



The following shows the display items and input restrictions for the Output definition file dialog box:

Specify the default values for authentication definitions specified in custom event jobs

Select this check box to output the authentication definition name selected from the pull-down menu as the default authentication definitions for custom event jobs.

Export button

Clicking this button outputs the service linkage monitoring job definition information file (`slmonjobdef.txt`) for registering custom event jobs. Do not change the output content of the service linkage monitoring job definition information file. Note that depending on the editor software, the character code, line break code, and existence of BOM might change simply by resaving the file.

If the content of the file is invalid, for example, when a BOM is assigned, a KNBB4511-E error occurs when executing the `ajscsajobreg` command for custom event job registration, and the processing fails.

Cancel button

Close the dialog box without doing anything.

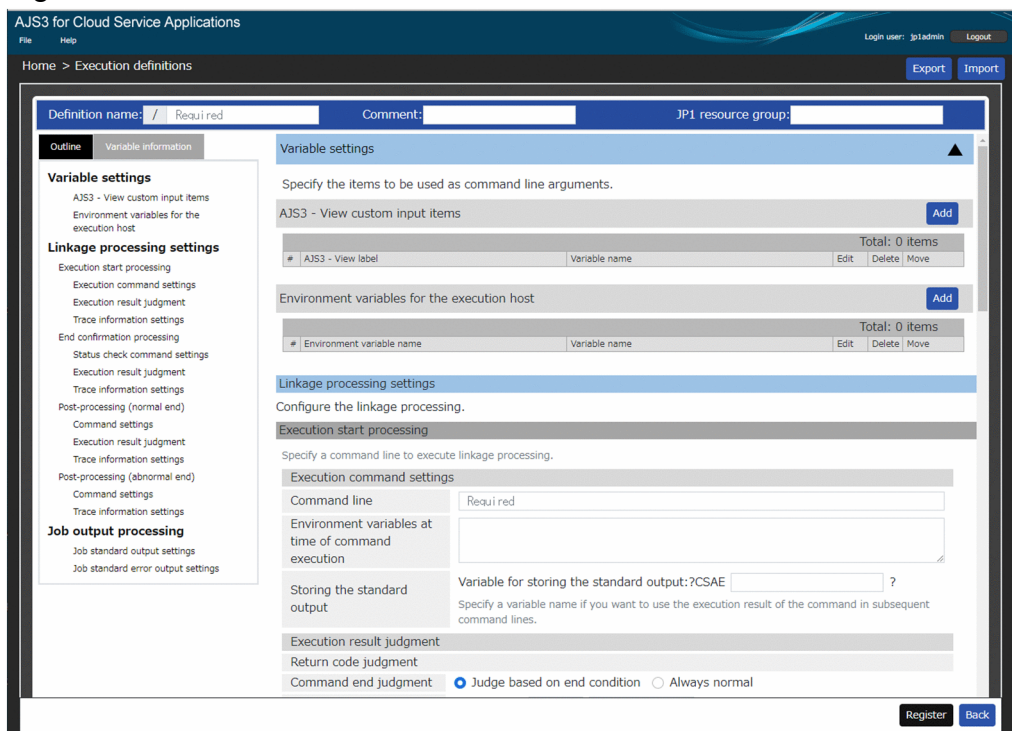
No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Default value for authentication definitions specified in custom event jobs	List box	Specify the registered authentication definition.	Required [#]	None

[#]: In case of specifying a default value of the authentication definition.

7.1.8 Execution definitions window

In the Execution definitions window, you can view and edit execution definitions in detail.

Figure 7–9: Execution definitions window



The following shows the display items and input restrictions for the Execution definitions window:

Definition name

Enter the definition name of the execution definition information. It is saved in the format of */definition-name*. It cannot be changed when editing.

Comment

Display the comment of the execution definition information.

JP1 resource group

Display the JP1 resource group of the execution definition information.

Outline tab

This tab shows the outline of the items in the right-hand definition area in a tree format. Clicking an item in the outline jumps to its corresponding item in the right-hand definition area.

Cautionary note

With an item hidden in the right-hand definition area, clicking the corresponding item in the outline does not jump to the item. Show in advance the hidden item in the right-hand definition area.

Variable information tab

Displays the variable information defined by each item in the definition area on the right side and the variable information that is reserved by the system and available by default.

Export button

Clicking this button outputs the execution information being displayed as the execution definition file (`slexecdefExport.txt`). This file will be output to the download folder set by the Web browser. For details about an execution definitions file, see *F.2 Execution definition file*.



Note

Even during input of execution definitions, an execution definition file can be exported.

Import button

Click this button to display the Open dialog allowing you to select an execution definition file to be reflected to the screen. Select an execution definition file. It will be reflected on the Execution definitions screen.

For details about the format of an execution definition file, see [F.2 Execution definition file](#).



Note

Even during input of execution definitions, an execution definition file can be imported.

Register button

Click this button to register the execution definitions, which have been input on the Execution definitions screen with JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed. If an error occurs, the item with the error is highlighted.

Back button

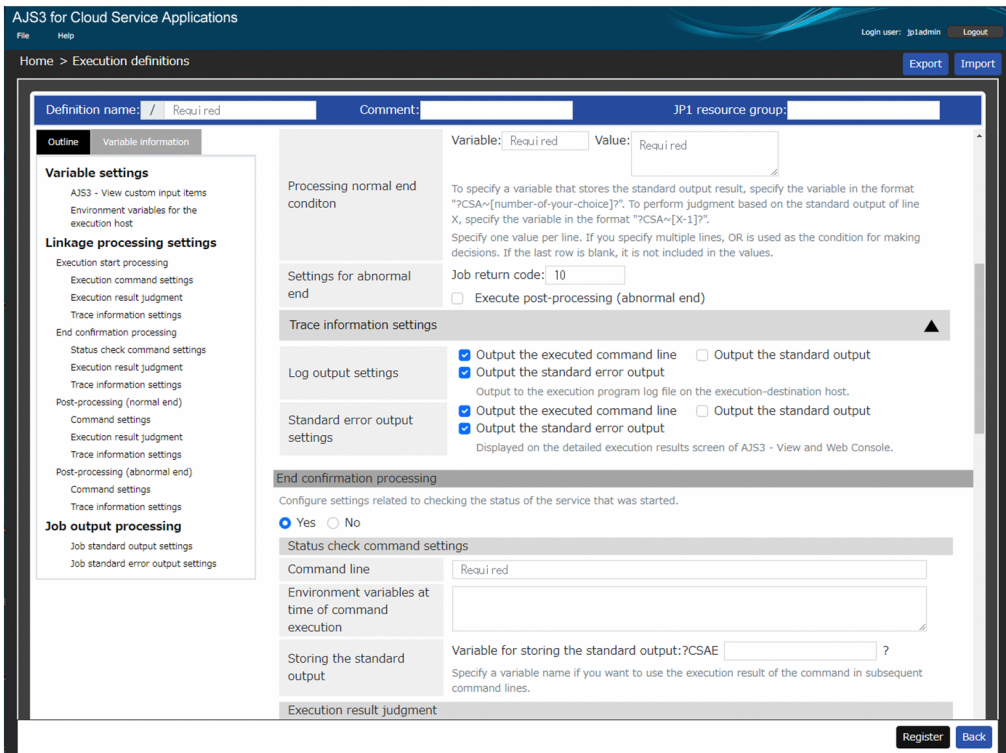
Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes. Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA

(1) Variable settings

This section explains about **Variable settings** in the Execution definitions window.

Figure 7–10: Variable settings in the Execution definitions window



The following shows the display items for **Variable settings**:

AJS3 - View custom input items

Display added variables and the list of AJS3 - View label name.

Add button

Click this button to open the Setting variables dialog box. Up to 15 variables can be added. For details about this dialog, see [7.1.8\(4\) Setting variables dialog box](#).

Delete button

Click this button to delete the variable for the selected row.

Edit button

Click this button to open the Setting variables dialog box with the variable for the selected row. For details about this dialog, see [7.1.8\(4\) Setting variables dialog box](#).

↑ button

Move the variable in the selected row one row up.

↓ button

Move the variable in the selected row one row down.

Environment variables for the execution host

Display added variables and list of environment variables.

Add button

Click this button to open the Setting variables dialog box. Up to 32 variables can be added. For details about this dialog, see [7.1.8\(4\) Setting variables dialog box](#).

Delete button

Click this button to delete the variable for the selected row.

Edit button

Click this button to open the Setting variables dialog box with the variable for the selected row. For details about this dialog, see 7.1.8(4) *Setting variables dialog box*.

↑ button

Move the variable in the selected row one row up.

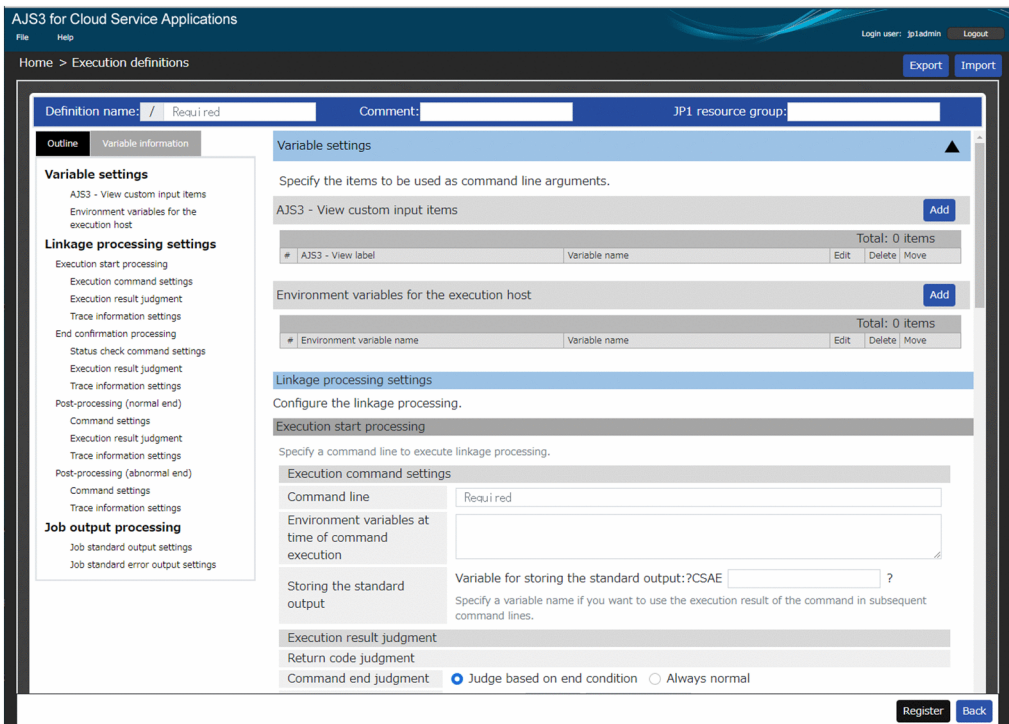
↓ button

Move the variable in the selected row one row down.

(2) Linkage processing settings

This section explains about **Linkage processing settings** in the Execution definitions window.

Figure 7–11: Linkage processing settings in the Execution definitions window



AJS3 for Cloud Service Applications

File Help Login user: jp1admin Logout

Home > Execution definitions

Export Import

Definition name: / Requi red Comment: JP1 resource group:

Outline Variable information

Variable settings
 AJS3 - View custom input items
 Environment variables for the execution host

Linkage processing settings
 Execution start processing
 Execution command settings
 Execution result judgment
 Trace information settings
 End confirmation processing
 Status check command settings
 Execution result judgment
 Trace information settings
 Post-processing (normal end)
 Command settings
 Execution result judgment
 Trace information settings
 Post-processing (abnormal end)
 Command settings
 Trace information settings

Job output processing
 Job standard output settings
 Job standard error output settings

Processing normal end condition
 Variable: Requi red Value: Requi red
 To specify a variable that stores the standard output result, specify the variable in the format "?CSA~[number-of-your-choice]?". To perform judgment based on the standard output of line X, specify the variable in the format "?CSA~[X-1]?". Specify one value per line. If you specify multiple lines, OR is used as the condition for making decisions. If the last row is blank, it is not included in the values.

Settings for abnormal end
 Job return code: 10
 Execute post-processing (abnormal end)

Trace information settings
 Output the executed command line Output the standard output
 Output the standard error output
 Output to the execution program log file on the execution-destination host.

Log output settings
 Output the executed command line Output the standard output
 Output the standard error output
 Displayed on the detailed execution results screen of AJS3 - View and Web Console.

Standard error output settings

End confirmation processing
 Configure settings related to checking the status of the service that was started.
 Yes No

Status check command settings
 Command line: Requi red
 Environment variables at time of command execution

Storing the standard output
 Variable for storing the standard output: ?CSAE [] ?
 Specify a variable name if you want to use the execution result of the command in subsequent command lines.

Execution result judgment

Register Back

AJS3 for Cloud Service Applications

File Help Login user: jp1admin Logout

Home > Execution definitions

Export Import

Definition name: / Requi red Comment: JP1 resource group:

Outline Variable information

Variable settings
 AJS3 - View custom input items
 Environment variables for the execution host

Linkage processing settings
 Execution start processing
 Execution command settings
 Execution result judgment
 Trace information settings
 End confirmation processing
 Status check command settings
 Execution result judgment
 Trace information settings
 Post-processing (normal end)
 Command settings
 Execution result judgment
 Trace information settings
 Post-processing (abnormal end)
 Command settings
 Trace information settings

Job output processing
 Job standard output settings
 Job standard error output settings

Specify whether to end the check immediately or to continue the check if the status check command fails.

Return code judgment
 Command end judgment: Judge based on end condition Always normal
 Abnormal end condition: Return code: > 0
 Settings for abnormal end: Job return code: 10
 Execute post-processing (abnormal end)

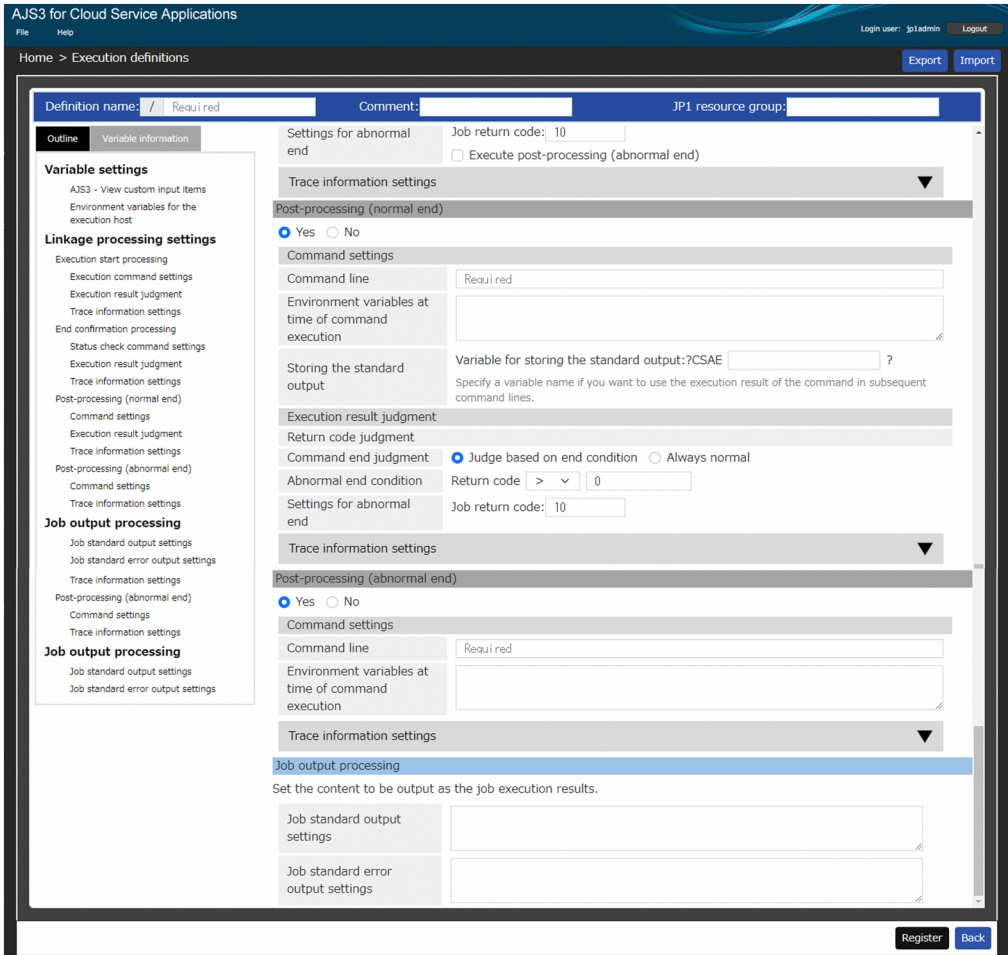
Output content judgment (Standard output)
 Command end judgment: Judge based on end condition Always normal
 Variable: Requi red Value: Requi red
 To specify a variable that stores the standard output result, specify the variable in the format "?CSA~[number-of-your-choice]?". To perform judgment based on the standard output of line X, specify the variable in the format "?CSA~[X-1]?". Specify one value per line. If you specify multiple lines, OR is used as the condition for making decisions. If the last row is blank, it is not included in the values.

Processing normal end condition
 Yes No

Retry settings
 Value of the retry condition: Requi red
 Specify one value per line. If you specify multiple lines, OR is used as the condition for making decisions. If the last row is blank, it is not included in the values.
 If neither the normal end condition nor the retry condition is met, processing ends abnormally in accordance with [Settings for abnormal end].
 Repeat interval: 0 minutes
 Number of times to repeat: 1 times
 Total time: 0minutes
 Settings at end of repeat: Job return code: 10
 Execute post-processing (abnormal end)

Processing continuation conditions

Register Back



The following shows the display items and input restrictions for the Linkage processing settings window:

(a) Execution start processing

■ Execution command settings

Command line

Enter the command line to run.

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

Storing the standard output - Variable for storing the standard output

Enter a variable name in the *?CSAExxxx?* format where the standard output details are stored for passing. Replace *xxxx* with a value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item. Also, specify "@CSA(characters-to-escape)ASC@" at locations where	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	escaping is required. For details, see section <i>4.3.3 Escaping a command line for cloud service linkage information</i> .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None
3	Variable for storing the standard output	Text box	Character string of 58 bytes or less. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Not required	None

■ Execution result judgment

Return code judgment - Command end judgment

Select operation at the end of a command from either of the following.

- Judge based on the end condition
Judge the execution result as normal or abnormal based on the return code.
- Always normal
Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the execution command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the job.

Execute post-processing (abnormal end)

Select this item when executing the processing set for **Post-processing (abnormal end)** before the end of the job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

Judgment of the output content (standard output) - Command end judgment

Select operation at the end of a command from either of the following.

- Judge based on the end condition
Judge the execution result as normal or abnormal based on the standard output details output by the command.
- Always normal
Judge the execution result always as normal regardless of the standard output details. When this item is selected, **Processing normal end condition** and **Settings for abnormal end** are hidden.

Processing normal end condition

Set the variable and its values for judging the normal end condition.

Variable

Enter a variable for judging the normal end condition in the ?CSAxxxxxx [YYYY] ? or ?CSAxxxxx? format. Specify the YYYY with a value one less than the number of rows you want to use for judgment of the standard output. Even in the case of only one row, the YYYY needs to be specified (0 should be specified in such a case).

Value

Enter up to 10 values that match the value of the specified variable. Multiple values can be specified by entering a line break for each one. When the value matches the value stored in the specified variable, the processing is judged as normal end.

Settings for abnormal end

Set the operation when the processing normal end condition is not satisfied.

Job return code

Enter the return code of the job.

Execute post-processing (abnormal end)

Select this item when executing the processing set for **Post-processing (abnormal end)** before the end of the job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Variable	Text box	Character string of 70 bytes or less. The variable can be specified in the ?CSAxxxxxx [YYYY] ? or ?CSAxxxxx? format. The characters that can be specified for xxxxxx and YYYY are as follows. xxxxxx: A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) YYYY: 0 to 9 (Arabic numbers)	Required	None
2	Value	Text box	Character string within 1,023 bytes. No line break is counted as part of the character string above. A tab character can also be specified. Up to 1,032 characters can be entered.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
2	Value	Text box	You can specify a variable in this input item.	Required	None
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

■ Trace information settings

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(b) End confirmation processing

To perform the end confirmation processing of the service executed for the execution start processing, select **Yes** and set the items below. If **No** is selected, the items below are not shown.

■ Status check command settings

Command line

Enter the command line to run.

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

Storing the standard output - Variable for storing the standard output

Enter a variable name in the *?CSAExxx?* format where the standard output details are stored for passing. Replace *xxx* with a value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	A tab character can also be specified. You can specify a variable in this input item. Also, specify "@CSA(characters-to-escape)ASC@" at locations where escaping is required. For details, see section 4.3.3 Escaping a command line for cloud service linkage information .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None
3	Variable for storing the standard output	Text box	Character string of 58 bytes or less. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Not required	None

■ Execution result judgment

Return code judgment - Command end judgment

Select operation at the end of a command from either of the following.

- Judge based on the end condition
Judge the execution result as normal or abnormal based on the return code.
- Always normal
Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the status check command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the job.

Execute post-processing (abnormal end)

Select this item when executing the processing set for **Post-processing (abnormal end)** before the end of the job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (! =), less than (<), more than (>), equal to	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

Judgment of the output content (standard output) - Command end judgment

Select operation at the end of a command from either of the following.

- Judge based on the end condition

Judge the execution result as normal or abnormal and whether to retry the processing based on the standard output details output by the command.

- Always normal

Judge the execution result always as normal regardless of the standard output details. When this item is selected, the following are hidden: **Processing normal end condition**, **Retry settings**, and **Settings for abnormal end**.

Processing normal end condition

Set the variables and their values for judging the normal end condition and processing continuity condition.

Variable

Enter a variable name for judging the normal end condition and processing continuity condition in the ?CSAxxxxxx [YYYY] ? or ?CSAxxxxxx? format. Specify the YYYY with a value one less than the number of rows you want to use for judgment of the standard output. Even in the case of only one row, the YYYY needs to be specified (0 in such a case).

Value

Enter up to 10 values that match the value of the specified variable. Multiple values can be specified by entering a line break for each one. When the value matches the value stored in the specified variable, the processing is judged as normal end.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Variable for processing normal end condition	Text box	Character string of 70 bytes or less. The variable can be specified in the ?CSAxxxxxx [YYYY] ? or ?CSAxxxxxx? format. The characters that can be specified for xxxxxx and YYYY are as follows. xxxxxx: A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) YYYY: 0 to 9 (Arabic numbers)	Required	None
2	Value for processing normal end condition	Text box	Character string within 1,023 bytes. No line break is counted as part of the character string above. A tab character can also be specified. Up to 1,032 characters can be entered.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
2	Value for processing normal end condition	Text box	You can specify a variable in this input item.	Required	None

Retry settings

Select whether to retry the processing based on the standard output details of the command. To retry the processing, select **Yes** and set the **Processing continuation conditions**. If **No** is selected, the **Processing continuation conditions** is not shown.

Processing continuation conditions

Enter conditions for the continuing operation.

Value of the retry condition

Enter up to 10 values that match the value of the variable of the specified normal end condition. Multiple values can be specified by entering a line break for each one. When the value matches the value stored in the specified variable, re-execute the status check command after the **Repeat interval**.

Repeat interval

Enter an interval for repeated execution.

Number of times to repeat

Enter the number of times of repeated execution.

Total time

This item displays the total time to be taken for the retry of the end confirmation processing based on the **Repeat interval** and **Number of times to repeat**. For a value outside the range of input restriction, - is shown.

Note that the total time includes neither the execution time of the status check command nor any other processing time.

Settings at end of repeat - Job return code

Enter the return code of the job when the processing has been performed for the specified number of times.

Settings at end of repeat - Execute post-processing (abnormal end)

Select this item when executing the processing set for **Post-processing (abnormal end)** before the end of the job in the case where the processing has been performed for the specified number of times.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Value of the retry condition	Text box	Character string within 1,023 bytes. No line break is counted as part of the character string above. A tab character can also be specified. Up to 1,032 characters can be entered. You can specify a variable in this input item.	Required	None
2	Repeat interval	Text box	A numerical value between 0 and 10. The unit is minutes.	Required	None
3	Number of times to repeat	Text box	A numerical value between 1 and 2,880.	Required	None
4	Total time	--	A numerical value between 1 and 2,880.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
4	Total time	--	The unit is minutes. This item displays the value of the product of the repeat interval and the repeat count.	Required	None
5	Job return code	Text box	A numerical value between 1 and 50.	Required	None

Settings for abnormal end

Set the operation when neither the normal end condition nor the processing continuity condition is met.

Job return code

Enter the return code of the job.

Execute post-processing (abnormal end)

Select this item when executing the processing set for **Post-processing (abnormal end)** before the end of the job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Job return code	Text box	A numerical value between 1 and 50.	Required	None

■ Trace information settings

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(c) Post-processing (normal end)

To perform post-processing after normal termination, select **Yes** and set the following items. If **No** is selected, the items below are not shown.

■ Command settings

Command line

Enter the command line to run.

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

Storing the standard output - Variable for storing the standard output

Enter a variable name in the *?CSAExxxx?* format where the standard output details are stored for passing. Replace *xxxx* with a value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item. Also, specify "@CSA(characters-to-escape)ASC@" at locations where escaping is required. For details, see section 4.3.3 <i>Escaping a command line for cloud service linkage information</i> .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None
3	Variable for storing the standard output	Text box	Character string of 58 bytes or less. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Not required	None

■ Execution result judgment

Return code judgment - Command end judgment

Select operation at the end of a command from either of the following.

- Judge based on the end condition
Judge the execution result as normal or abnormal based on the return code.
- Always normal
Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the status check command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

■ Trace information settings

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(d) Post-processing (abnormal end)

To perform post-processing after abnormal termination, select **Yes** and set the following items. If **No** is selected, the items below are not shown.

■ Command settings

Command line

Enter the command line to run.

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item. Also, specify "@CSA(characters-to-escape)ASC@" at locations where escaping is required. For details, see section 4.3.3 Escaping a command line for cloud service linkage information .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None

■ Trace information settings

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

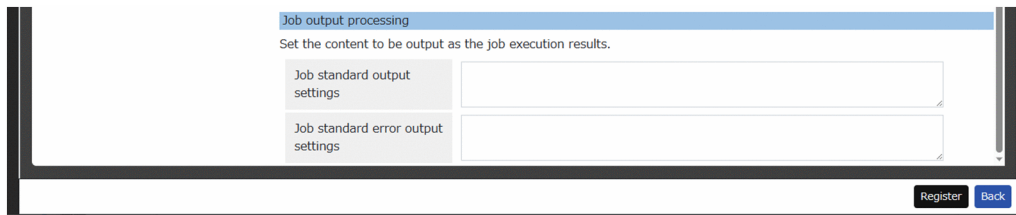
Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(3) Job output processing

This section explains about **Job output processing** in the Execution definitions window.

Figure 7–12: Job output processing in the Execution definitions window



The following shows the display items and input restrictions for the Job output processing window:

Job standard output settings

Enter the contents to be output to the standard output as the job execution result.

Job standard error output settings

Enter the contents to be output to the standard error output as the job execution result.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Job standard output settings	Text box	Character string within 1,023 bytes. Line breaks are also counted in the above string. A tab character can also be specified. You can specify a variable in this input item.	Not required	None
2	Job standard error output settings	Text box	Character string within 1,023 bytes. Line breaks are also counted in the above string. You can specify a variable in this input item.	Not required	None

(4) Setting variables dialog box

The Setting variables dialog is displayed for adding a new variable by pressing **Add** or editing an existing variable by pressing **Edit** in the **AJS3 - View custom input items** or **Environment variables for the execution host**.

Figure 7–13: Setting variables dialog box for the AJS3 - View custom input items

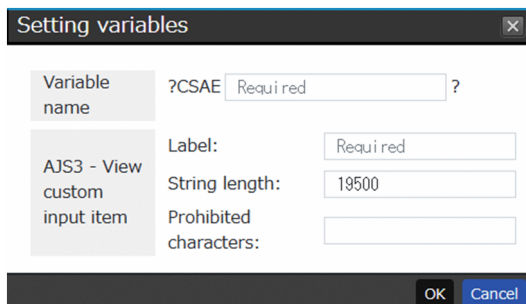
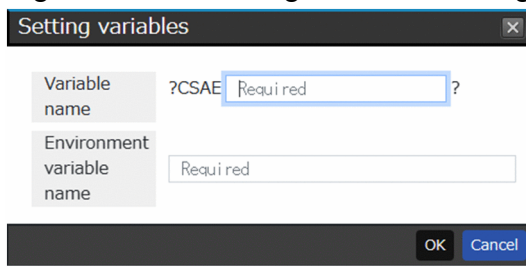


Figure 7–14: Setting variables dialog box for the Environment variables for the execution host



The following shows the display items and input restrictions for the Setting variables dialog box:

Variable name

When the system is started with the **AJS3 - View custom input items**, enter a variable name in the `?CSAExxxx?` format with `xxxx` replaced with the desired value. This variable stores the standard output details entered on the details definition screen of the service linkage job of JP1/AJS3 - View and sets information to be passed. When the system is started with the **Environment variables for the execution host**, enter the name of the variable that stores the value of the environment variable set on the execution host and sets the information to be passed.

AJS3 - View custom input items

This item is displayed only when you click the **Add** or **Edit** button in **AJS3 - View custom input items**.

Label

Enter the label name of the input item on the detailed definition screen of the service linkage job of JP1/AJS3 - View.

String length

Enter the input string length in the detail definition screen of the service linkage job of JP1/AJS3 - View.

Prohibited characters

Enter characters with a regular expression that are to be prohibited to input on the details definition screen of service linkage jobs of JP1/AJS3 - View.

Available regular expressions are those that can be used in the .NET Framework. For details, see the related documents provided by Microsoft Corporation.

Environment variable name

This item is displayed only when **Add** or **Edit** is pressed in **Environment variables for the execution host**.

Enter an environment variable name to be stored in the variable.

OK button

Click this button to register the variable with the entered information.

Cancel button

Closes the Setting variable dialog box without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Variable name	Text box	Character string within 58 bytes. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Required	None
2	Label	Text box	Character string within 60 bytes.	Required	None
3	String length	Text box	A numerical value between 1 and 19,500.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
4	Prohibited characters	Text box	Character string within 95 bytes.	Not required	None
5	Environment variable name	Text box	Character string within 64 bytes.	Required	None

7.1.9 Object monitoring definition window

In the Object monitoring definition window, you can view and edit object monitoring definitions in detail.

Figure 7–15: Object monitoring definition window

The following shows the display items and input restrictions for the Object monitoring definition window:

Definition name

Enter the definition name of the monitoring definition information. It is saved in the format of */definition-name*. It cannot be changed when editing.

Comment

Enter a description of monitoring definition information.

JP1 resource group

Enter the JP1 resource group of the monitoring definition information.

Outline tab

This tab shows the outline of the items in the right-hand definition area in a tree format. Clicking an item in the outline jumps to its corresponding item in the right-hand definition area.

Cautionary note

With an item hidden in the right-hand definition area, clicking the corresponding item in the outline does not jump to the item. Open the hidden item in the right-hand definition area in advance.

Variable information tab

Displays the variable information defined by each item in the definition area on the right side and the variable information that is reserved by the system and available by default.

Export button

Clicking this button outputs the monitoring information being displayed as the service linkage objects monitoring definition file (`slobjmondefExport.txt`). This file will be output to the download folder set by the Web browser.

For details about the service linkage objects monitoring definition file, see [G.1 Service linkage objects monitoring definition file](#).



Note

Even during input of monitoring definitions, a service linkage objects monitoring definition file can be exported.

Import button

Click this button to display the Open dialog allowing you to select a service linkage objects monitoring definition file to be reflected to the screen. Select a service linkage objects monitoring definition file. It will be reflected on the Object monitoring definition window.

For details about the format of service linkage objects monitoring definition files that can be imported, see [G.1 Service linkage objects monitoring definition file](#).



Note

Even during input of monitoring definitions, a service linkage objects monitoring definition file can be imported.

Register button

Click this button to register monitoring information input in the Object monitoring definition window to JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed.

If an error occurs, the item with the error is highlighted.

Back button

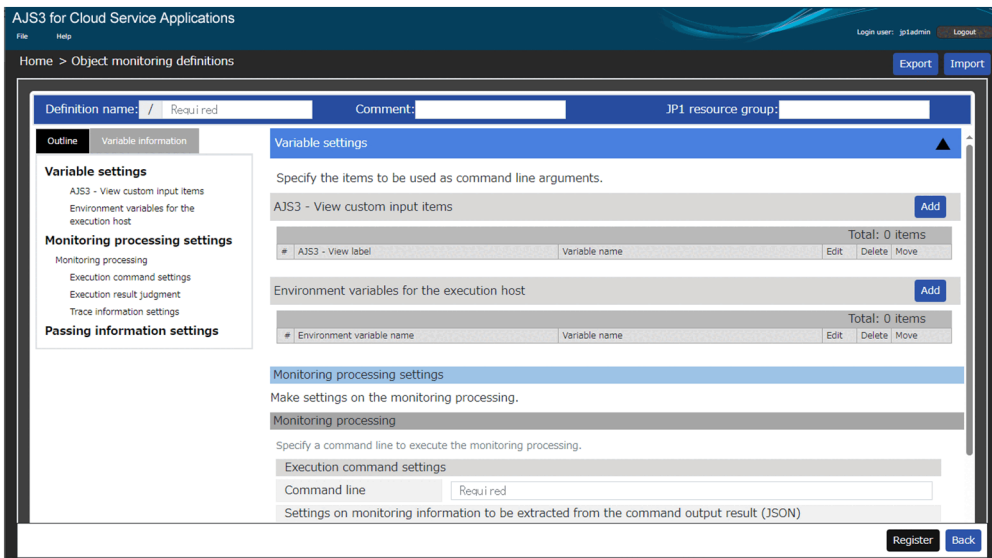
Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes. Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA

(1) Variable settings

This section describes the **Variable settings** in the Object monitoring definition window.

Figure 7–16: Variable settings in the Object monitoring definition window



The following shows the display items for **Variable settings**.

AJS3 - View custom input items

Display added variables and the list of AJS3 - View label names.

Add button

Click this button to open the Setting variables dialog box. Up to 15 variables can be added. For details about this dialog, see [7.1.9\(3\) Setting variables dialog box](#).

Delete button

Click this button to delete the variable for the selected row.

Edit button

Click this button to open the Setting variables dialog box with the variable for the selected row. For details about this dialog, see [7.1.9\(3\) Setting variables dialog box](#).

↑ button

Move the variable in the selected row one row up.

↓ button

Move the variable in the selected row one row down.

Environment variables for the execution host

Display added variables and a list of environment variables.

Add button

Click this button to open the Setting variables dialog box. Up to 32 variables can be added. For details about this dialog, see [7.1.9\(3\) Setting variables dialog box](#).

Delete button

Click this button to delete the variable for the selected row.

Edit button

Click this button to open the Setting variables dialog box for the selected row. For details about this dialog, see [7.1.9\(3\) Setting variables dialog box](#).

↑ button

Move the variable in the selected row one row up.

↓ button

Move the variable in the selected row one row down.

(2) Monitoring processing settings

This section describes the **Monitoring processing settings** in the Object monitoring definition window.

Figure 7–17: Monitoring processing settings in the Object monitoring definition window

Home > Object monitoring definitions

Export Import

Definition name: Required Comment: JP1 resource group:

Outline Variable information

Variable settings

- AJS3 - View custom input items
- Environment variables for the execution host

Monitoring processing settings

- Monitoring processing
- Execution command settings
- Execution result judgment
- Trace information settings

Passing information settings

Monitoring processing settings

Make settings on the monitoring processing.

Monitoring processing

Specify a command line to execute the monitoring processing.

Execution command settings

Command line Required

Settings on monitoring information to be extracted from the command output result (JSON)

Specify the extraction processing to save data from JSON to each item of monitoring information.

Variable for storing the standard output JMESPath query syntax

Object name ?CSAONAME? Required

Update monitoring target 1 ?CSAONF01?

Update monitoring target 2 ?CSAONF02?

Update monitoring target 3 ?CSAONF03?

Environment variables at time of command execution

Execution result judgment

Return code judgment

Abnormality judgment condition Return code > 0

Settings for abnormal end Abnormal end occurs Monitoring continues

Job return code 110

Output settings for detailed execution results Output the executed command line Output the standard output Output the standard error output

Displayed on the detailed execution results screen of AJS3 - View and Web Console.

Output the standard output

Log output settings Output to the execution program log file on the execution-destination host.

Register Back

Execution command settings

Execution result judgment

Trace information settings

Passing information settings

Specify values to be passed on to each passing information name for the custom event job.

Name of passing information to be used as the storage destination Value

Name of passing information to be used as the storage destination	Value
OBJECT01	?CSAONAME?
OBJECT02	
OBJECT03	
OBJECT04	
OBJECT05	
OBJECT06	
OBJECT07	
OBJECT08	
OBJECT09	
OBJECT10	

Register Back

The following shows the display items and input restrictions for **Monitoring processing settings**.

(a) Monitoring processing

■ Execution command settings

Command line

Enter the command line to run.

Settings on monitoring information to be extracted from the command output result (JSON)

Enter the JMESPath query syntax to extract the object name and information subject to update monitoring from the output results of the executed command.

For details about content specified to this item, see [6.2.1\(3\) Processing for extracting object information on the cloud service](#).

Environment variables at time of command execution

Enter an environment variable to be used for command line execution in *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item. Also, specify @CSA (<i>characters-to-escape</i>) ASC@ at locations where escaping is required. For details, see 4.3.3 Escaping a command line for cloud service linkage information .	Required	None
2	Object name	Text box	Character string within 256 bytes. Double quotes (") and single quotes (') cannot be used.	Required	None
3	Update monitoring target 1	Text box	Character string within 256 bytes. Double quotes (") and single quotes (') cannot be used.	Not required	None
4	Update monitoring target 2	Text box	Character string within 256 bytes. Double quotes (") and single quotes (') cannot be used.	Not required	None
5	Update monitoring target 3	Text box	Character string within 256 bytes. Double quotes (") and single quotes (') cannot be used.	Not required	None
6	Environment variables at time of command execution	Text box	Character string within 20,479 bytes. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None

■ Execution result judgment

Return code judgment - Abnormality judgment condition

Enter the abnormality judgment condition of the return code of the execution command.

Settings for abnormal end

Select the response when an abnormality occurs from the following:

- **Abnormal end occurs**

Abnormally end the service linkage object monitoring job.

- **Monitoring continues**

Continue monitoring regardless of the return code. If this item is selected, **Job return code**, **Output settings for detailed execution results**, and **Log output settings** are hidden from view.

Job return code

Enter the return code of the job when ended abnormally.

Output settings for detailed execution results

Select content to be output to detailed execution results when a job ends abnormally.

Output the executed command line

Select whether to output the executed command to detailed execution results.

Output the standard output

Select whether to output the standard output of executed commands to detailed execution results.

Output the standard error output

Select whether to output the standard error output of executed commands to detailed execution results.

Log output settings

Select content to be output to the log when a job ends abnormally.

Output the standard output

Select whether to output the standard output of executed commands to the log.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Job return code	Text box	A numerical value between 101 and 150.	Required	110

■ Trace information settings

Log output settings

Configure settings for output to the service linkage objects monitoring job log file for each monitoring interval. For details about service linkage monitoring job logs, see [9.2.7 Service Linkage Monitoring Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

(b) Passing information settings

Enter the values stored for passing information names OBJECT01 to OBJECT10 in a custom event job when the service linkage objects monitoring job ends normally. Variables can be specified for all items.

No.	Name of passing information to be used as the storage destination	Input format	Input restriction	Required/Not required	Assumed value
1	OBJECT01	Text box	Character string within 256 bytes.	Not required	? CSAONAME?
2	OBJECT02	Text box	Character string within 256 bytes.	Not required	None
3	OBJECT03	Text box	Character string within 256 bytes.	Not required	None
4	OBJECT04	Text box	Character string within 256 bytes.	Not required	None
5	OBJECT05	Text box	Character string within 256 bytes.	Not required	None
6	OBJECT06	Text box	Character string within 256 bytes.	Not required	None
7	OBJECT07	Text box	Character string within 256 bytes.	Not required	None
8	OBJECT08	Text box	Character string within 256 bytes.	Not required	None
9	OBJECT09	Text box	Character string within 256 bytes.	Not required	None
10	OBJECT10	Text box	Character string within 256 bytes.	Not required	None

(3) Setting variables dialog box

The Setting variables dialog box is displayed for adding a new variable by clicking **Add** or editing an existing variable by clicking **Edit** in the **AJS3 - View custom input items** or **Environment variables for the execution host**.

Figure 7–18: Setting variables dialog box for the AJS3 - View custom input items

Figure 7–19: Setting variables dialog box for the Environment variables for the execution host

The following shows the display items and input restrictions for the Setting variables dialog box:

Variable name

When the system is started with the **AJS3 - View custom input items**, enter a variable name in the `?CSAOxxxx?` format with `xxxx` replaced with the desired value. This variable stores details entered on the details definition screen of the service linkage job of JP1/AJS3 - View and sets information to be passed. When the system is started with the **Environment variables for the execution host**, enter the name of the variable that stores the value of the

environment variable set on the execution host for the service linkage objects monitoring job and sets the information to be passed.

AJS3 - View custom input item

This item is displayed only when you click the **Add** or **Edit** button in **AJS3 - View custom input items**.

Label

Enter the label name of the input item on the detailed definition screen of the service linkage objects monitoring job of JP1/AJS3 - View.

String length

Enter the input string length in the detailed definition screen of the service linkage objects monitoring job of JP1/AJS3 - View.

Prohibited characters

Enter characters with a regular expression that are to be prohibited to input on the detailed definition screen of the service linkage objects monitoring job of JP1/AJS3 - View.

Available regular expressions are those that can be used in the .NET Framework. For details, see the related documents provided by Microsoft Corporation.

Environment variable name

This item is displayed only when you click the **Add** or **Edit** button in **Environment variables for the execution host**.

Enter an environment variable name to be stored in the variable.

OK button

Click this button to register the variable with the entered information.

Cancel button

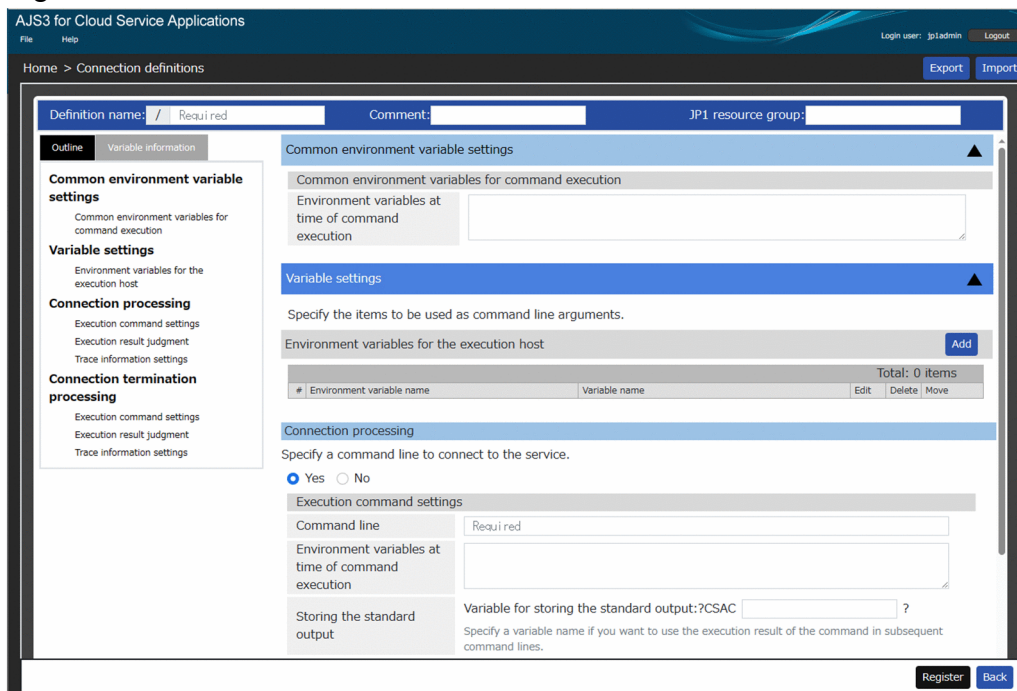
Closes the Setting variable dialog box without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Variable name	Text box	Character string within 58 bytes. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Required	None
2	Label	Text box	Character string within 60 bytes.	Required	None
3	String length	Text box	A numerical value between 1 and 12,000.	Required	12000
4	Prohibited characters	Text box	Character string within 95 bytes.	Not required	None
5	Environment variable name	Text box	Character string within 64 bytes.	Required	None

7.1.10 Connection definitions window

In the Connection definitions window, you can view and edit connection definitions in detail.

Figure 7–20: Connection definitions window



The following shows the display items and input restrictions for the Connection definitions window:

Definition name

Enter the definition name of the connection definition information. It is saved in the format of */definition-name*. It cannot be changed when editing.

Comment

Display the comment of the connection definition information.

JP1 resource group

Display the JP1 resource group of the connection definition information.

Outline tab

This tab shows the outline of the items in the right-hand definition area in a tree format. Clicking an item in the outline jumps to its corresponding item in the right-hand definition area.

Cautionary note

With an item hidden in the right-hand definition area, clicking the corresponding item in the outline does not jump to the item. Show in advance the hidden item in the right-hand definition area.

Variable information tab

Displays the variable information defined by each item in the definition area on the right side and the variable information that is reserved by the system and available by default.

Export button

Clicking this button outputs the connection information being displayed as the connection definition file (`slcondefExport.txt`). This file will be output to the download folder set by the Web browser.

For details about a connection definitions file, see *F.1 Connection definition file*.



Note

Even during input of connection definitions, a connection definition file can be exported.

Import button

Click this button to display the Open dialog allowing you to select a connection definition file to be reflected to the screen. Select a connection definition file. It will be reflected on the Connection definitions screen.

For details about the format of a connection definition file, see [F.1 Connection definition file](#).



Note

Even during input of connection definitions, a connection definition file can be imported.

Register button

Click this button to register the connection definitions, which have been input on the Connection definitions screen with JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed. If an error occurs, the item with the error is highlighted.

Back button

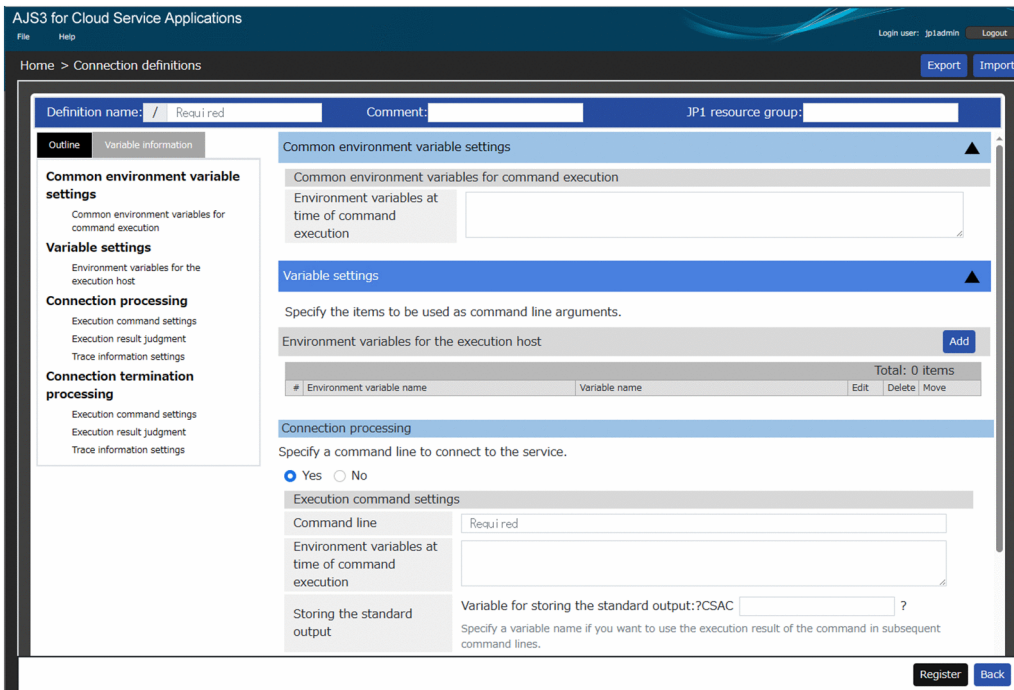
Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes. Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA

(1) Common environment variable settings

This section explains about **Common environment variable settings** in the Connection definitions window.

Figure 7–21: Common environment variable settings in the Connection definitions window



The following shows the display items for **Common environment variable setting**:

(a) Common environment variables for command execution

Environment variables at time of command execution

Enter an environment variable to be used for command line execution with connection definitions, execution definitions, and monitoring definitions commonly in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

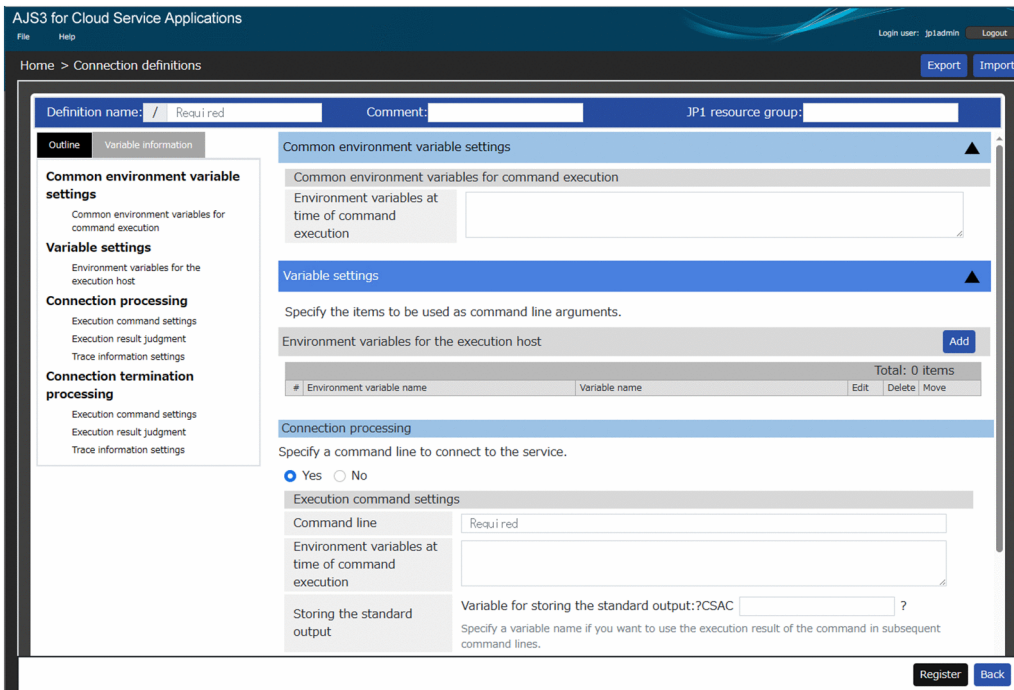
The following environment variable is prioritized over that set for this item: the environment variable set for **Environment variables at time of command execution** in the command line of each definition.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None

(2) Variable settings

This section explains about **Variable settings** in the Connection definitions window.

Figure 7–22: Variable settings in the Connection definitions window



The following shows the display items for **Variable settings**:

Environment variables for the execution host

Display added variables and the list of environment variables name.

Add button

Click this button to open the Setting variables dialog box. Up to 32 variables can be added. For details about this dialog, see [7.1.10\(5\) Setting variables dialog box](#).

Delete button

Click this button to delete the variable for the selected row.

Edit button

Click this button to open the Setting variables dialog box with the variable for the selected row. For details about this dialog, see [7.1.10\(5\) Setting variables dialog box](#).

↑ button

Move the variable in the selected row one row up.

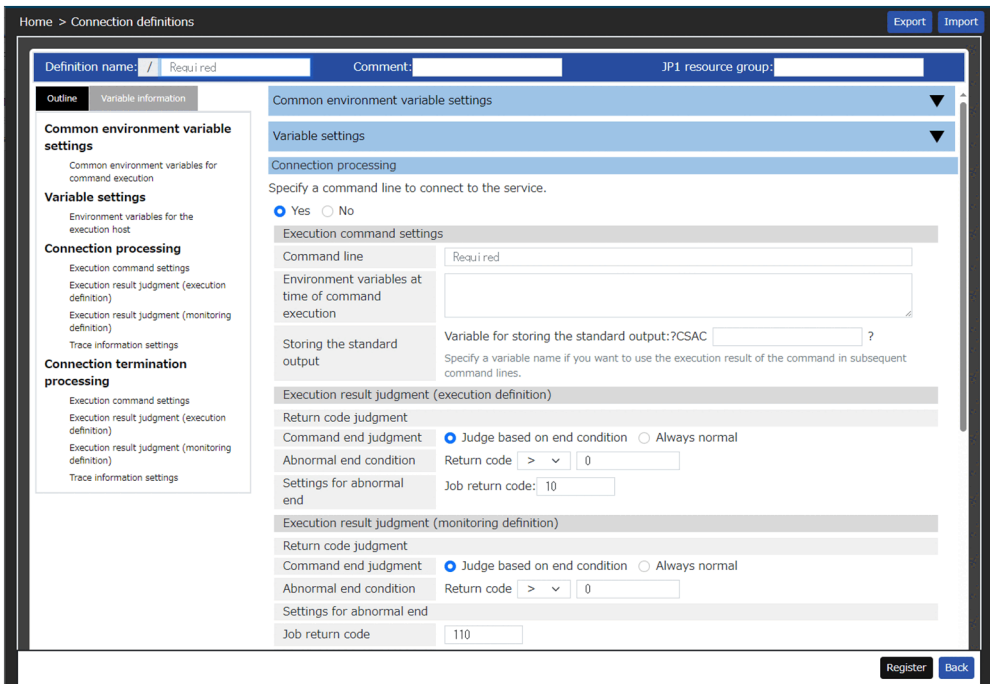
↓ button

Move the variable in the selected row one row down.

(3) Connection processing

This section explains about **Connection processing** in the Connection definitions window.

Figure 7–23: Connection processing in the Connection definitions window



When setting connection processing by specifying a command line for establishing a connection to a service, select **Yes** and set the items shown below. If **No** is selected, the items below are not shown.

The following shows the display items for **Connection processing**:

(a) Execution command settings

Command line

Enter the command line to run.

Command lines entered for this item are executed at the following times:

For service linkage jobs

Before **Execution start processing** of the execution definition

For service linkage monitoring jobs

Before executing the information acquisition command specified in **Monitoring processing** of the monitoring definition (executed at monitoring intervals)

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

Storing the standard output - Variable for storing the standard output

Enter a variable name in the *?CSACxxxx?* format where the standard output details are stored for passing. Replace *xxxx* with a value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Also, specify "@CSA(<i>characters-to-escape</i>)ASC@" at locations where escaping is required. For details, see section <i>4.3.3 Escaping a command line for cloud service linkage information</i> .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None
3	Variable for storing the standard output	Text box	Character string of 58 bytes or less. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Not required	None

(b) Execution result judgment (execution definition)

Return code judgment - Command end judgment

Select operation at the end of a connection command executed on the execution definition side from either of the following.

- **Judge based on end condition**

Judge the execution result as normal or abnormal based on the return code.

- **Always normal**

Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the execution command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the service linkage job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

(c) Execution result judgment (monitoring definition)

Return code judgment - Command end judgment

Select operation at the end of a connection command executed on the monitoring definition side from either of the following:

- **Judge based on end condition**

Judge the execution result as normal or abnormal based on the return code.

- **Always normal**

Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the execution command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the service linkage monitoring jobs.

Output settings for detailed execution results

Select the content to be output to detailed execution results when a service linkage monitoring job ends abnormally.

- **Output the executed command line**

Select whether to output the executed command line to detailed execution results.

- **Output the standard output**

Select whether to output the standard output of executed commands to detailed execution results.

- **Output the standard error output**

Select whether to output the standard error output of the executed command to detailed execution results.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None
3	Job return code	Text box	A numerical value between 101 and 150.	Required	None

(d) Trace information settings (execution definition)

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(e) Trace information settings (monitoring definition)

Log output settings

Configure settings for output to the service linkage monitoring job log file for each monitoring interval. The service linkage monitoring job log to be output is different depending on the type of service linkage monitoring job. For details about each type of log, see [9.2.7 Service Linkage Monitoring Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

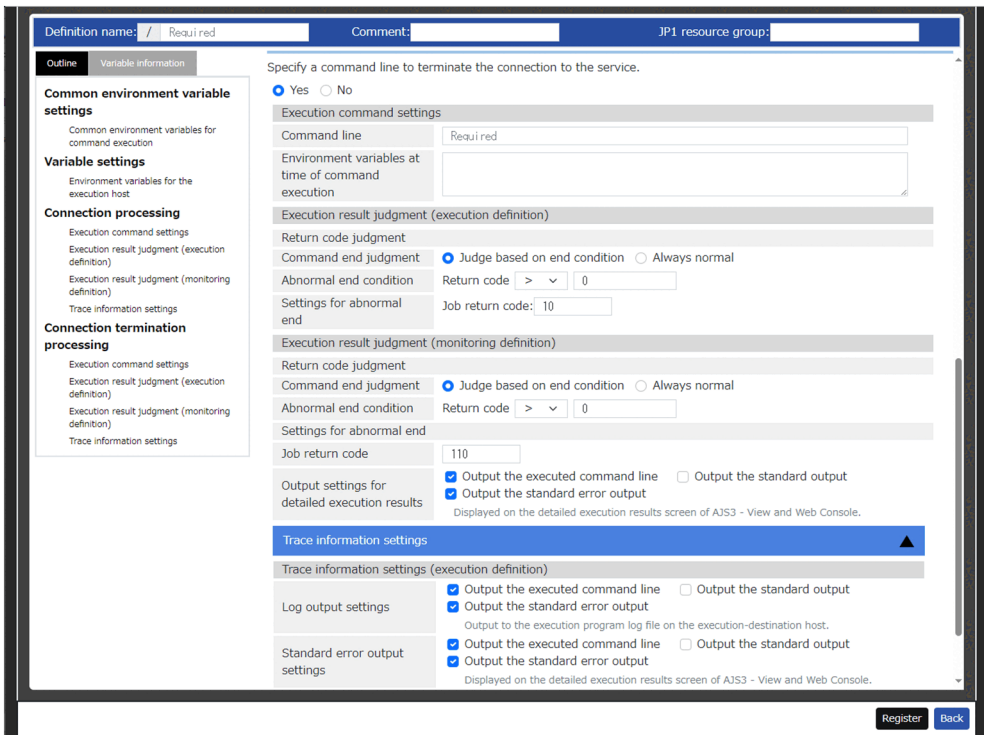
Output the standard error output

Select whether to output the standard error output of executed commands to the log.

(4) Connection termination processing

This section explains about **Connection termination processing** in the Connection definitions window.

Figure 7–24: Connection termination processing in the Connection definitions window



When setting disconnection processing by specifying a command line for disconnection from a service, select **Yes** and set the items shown below. If **No** is selected, the items below are not shown.

The following shows the display items for **Connection termination processing**:

(a) Execution command settings

Command line

Enter the command line to run.

Command lines entered for this item are executed at the following times:

For service linkage jobs

After all processes of the execution definition have ended

For service linkage monitoring jobs

After executing the information acquisition command specified in **Monitoring processing** of the monitoring definition (executed at monitoring intervals)

Environment variable at time of command execution

Enter an environment variable to be used for command line execution in the *environment-variable-name=environment-variable-value* format. When specifying multiple variables, enter a line break for each one.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	Character string within 1,023 bytes. A tab character can also be specified. You can specify a variable in this input item. Also, specify "@CSA(characters-to-escape)ASC@" at locations where	Required	None

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Command line	Text box	escaping is required. For details, see section <i>4.3.3 Escaping a command line for cloud service linkage information</i> .	Required	None
2	Environment variables at time of command execution	Text box	Character string of 20,479 bytes or less. No line break is counted as part of the character string above. A tab character can also be specified. Up to 27,304 characters can be entered. You can specify a variable in this input item.	Not required	None

(b) Execution result judgment (execution definition)

Return code judgment - Command end judgment

Select operation at the end of a connection termination command executed on the execution definition side from either of the following.

- **Judge based on end condition**

Judge the execution result as normal or abnormal based on the return code.

- **Always normal**

Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code of the execution command.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the service linkage job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None
3	Job return code	Text box	A numerical value between 1 and 50.	Required	None

(c) Execution result judgment (monitoring definition)

Return code judgment - Command end judgment

Select operation at the end of a connection termination command executed on the monitoring definition side from either of the following:

- **Judge based on end condition**

Judge the execution result as normal or abnormal based on the return code.

- **Always normal**

Judge the execution result always as normal regardless of the return code. When this item is selected, **Abnormal end condition** and **Settings for abnormal end** are hidden.

Abnormal end condition

Enter an abnormal end condition of the return code.

Settings for abnormal end

Set operation when the abnormal end condition is met.

Job return code

Enter the return code of the service linkage monitoring job.

Output settings for detailed execution results

Select content to be output to detailed execution results when a service linkage monitoring job ends abnormally.

- **Output the executed command line**

Select whether to output the executed command to detailed execution results.

- **Output the standard output**

Select whether to output the standard output of executed commands to detailed execution results.

- **Output the standard error output**

Select whether to output the standard error output of executed commands to detailed execution results.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Conditions for Abnormal end condition	List box	Select from the following. Equal to (=), not equal to (!=), less than (<), more than (>), equal to or less than (<=), equal to or more than (>=)	Required	None
2	Value for Abnormal end condition	Text box	A numerical value between 0 and 2,147,483,647.	Required	None
3	Job return code	Text box	A numerical value between 101 and 150.	Required	None

(d) Trace information settings (execution definition)

Log output settings

Configure settings for output to the service linkage job log file. For details about service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

Output the standard error output

Select whether to output the standard error output of executed commands to the log.

Standard error output settings

Sets the output to the standard error output.

Output the executed command line

Select whether to output the executed command line to the standard error output.

Output the standard output

Select whether to output the standard output of the executed command to the standard error output.

Output the standard error output

Select whether to output the standard error output of the executed command to the standard error output.

(e) Trace information settings (monitoring definition)

Log output settings

Configure settings for output to the service linkage monitoring job log file for each monitoring interval. The service linkage monitoring job log to be output is different depending on the type of service linkage monitoring job. For details about each type of log, see [9.2.7 Service Linkage Monitoring Job Log](#).

Output the executed command line

Select whether to output the executed command line to the log.

Output the standard output

Select whether to output the standard output of executed commands to the log.

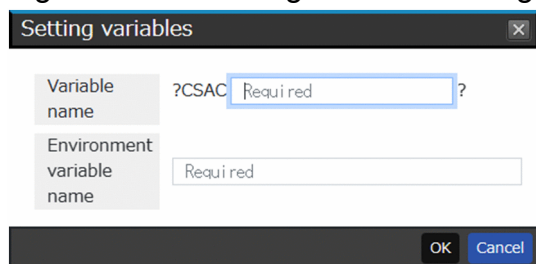
Output the standard error output

Select whether to output the standard error output of executed commands to the log.

(5) Setting variables dialog box

The Setting variables dialog is displayed for adding a new variable by pressing **Add** or editing an existing variable by pressing **Edit** in the **Environment variables for the execution host**.

Figure 7–25: Setting variables dialog box



The following shows the display items and input restrictions for the Setting variables dialog box:

Variable name

Enter the name of a variable, in the `?CSACxxxx?` format with `xxxx` replaced with a desired value that stores the value of the environment variable set on the execution host and sets the information to be passed.

Environment variable name

Enter an environment variable name to be stored in the variable.

OK button

Click this button to register the variable with the entered information.

Cancel button

Closes the Setting variable dialog box without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Variable name	Text box	Character string within 58 bytes. A to Z (uppercase alphabetical letters) and 0 to 9 (Arabic numbers) are available.	Required	None
2	Environment variable name	Text box	Character string within 64 bytes.	Required	None

7.1.11 Authentication definitions window

In the Authentication definitions window, you can view and edit authentication definitions in detail.

Figure 7–26: Authentication definitions window

The following shows the display items and input restrictions for the Authentication definitions window:

Definition name

Enter the definition name of the authentication definition information. It is saved in the format of */definition-name*. It cannot be changed when editing.

Comment

Display the comment of the authentication definition information.

JP1 resource group

Display the JP1 resource group of the authentication definition information.

Register button

Click this button to register the connection definitions, which have been input on the Authentication definitions screen with JP1/AJS3 for Cloud Service Applications. When registration is successfully completed, the Home window is displayed.

If an error occurs, the item with the error is highlighted.

Back button

Go to the Home window without doing anything.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Definition name	Text box	Character string of 1 to 30 bytes. Single-byte alphanumeric characters, - (hyphen), and _ (underscore) are available.	Required	None
2	Comment	Text box	Character string within 243 bytes.	Not required	None
3	JP1 resource group	Text box	Character string within 63 bytes. Single-byte alphanumeric characters and _ (underscores) are available.	Not required	JP1_CSA

(1) ID/user

Sets the ID and user information used to connect to the service.

The following shows the display items for **ID/user**:

Variable for storing the standard output

The variable name storing the ID and user information is fixed to ?CSAAIDINFO?.

Value

Enter a value to be set for the variable.

Update value

Select whether to update the value at the time of registration. With the item selected, the **Value** field is enabled. Without the item selected, the **Value** field is disabled.

This item must remain selected because the item is always updated at the time of new creation. With this item selected, the value is updated.

Comment

Enter a comment of the value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Value	Text box	Character string of 128 bytes or less. You can use an alphanumeric character (ASCII).	Required	None
2	Comment	Text box	Character string within 48 bytes.	Required	None

(2) Security information/password

Set security information and a password for connection with a service.

The following shows the display items for **Security information/password**:

Protect

The data are protected as security information. The selection status cannot be changed.

Variable for storing the standard output

The variable name storing the security information and password is fixed to ?CSAAPWDINFO?.

Value

Enter a value to be set for the variable.

Each input character is displayed with •.

Without the **Update value** selected, the field is always shown with ••• When the **Update value** is selected, the input characters are overwritten with null characters.

When editing, ••• is always displayed regardless of the value at the time of registration.

Update value

Select whether to update the value at the time of registration. With the item selected, the **Value** field is enabled.

Without the item selected, the **Value** field is disabled.

Comment

Enter a comment of the value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Value	Text box	Character string of 128 bytes or less. You can use an alphanumeric character (ASCII).	Required	None
2	Comment	Text box	Character string within 48 bytes.	Required	None

(3) Additional information item 1 to 3

Set other additional information to be used for connection with a service.

The following shows the display items and input restrictions of the **Additional information item 1** to **Additional information item 3**.

Protect

The data are protected as security information.

Variable for storing the standard output

The variable name storing additional information is fixed to ?CSAAINF1? through ?CSAAINF3?.

Value

Enter a value to be set for the variable. The display differs depending on whether **Protect** is selected or not.

- Without the **Protect** selected

The input characters are displayed as they are.

The input characters are displayed as they are regardless of whether the **Update value** is selected.

- With the **Protect** selected

Each input character is displayed with •.

Without the **Update value** selected, the field is always shown with ••• When the **Update value** is selected, the input characters are overwritten with null characters.

When editing the definition registered with the **Protect** selected, ••• is always displayed regardless of the value at the time of registration.

Update value

Select whether to update the value at the time of registration. With the item selected, the **Protect** is enabled and the **Value** field is enabled. Without the item selected, the **Value** and **Protect** are disabled.

Comment

Enter a comment of the value.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Value	Text box	Character string of 128 bytes or less. You can use an alphanumeric character (ASCII).	Required	None
2	Comment	Text box	Character string within 48 bytes.	Required	None

7.1.12 Notes on Web GUI

This section describes notes on the use of the Web GUI.

About OS limitations on command lines

When the execution host of service linkage jobs or service linkage monitoring jobs is on Windows, the number of characters that can be used is approximately 8,000 because there is a limitation on OS command lines.

Input value restrictions

Multibyte input characters, if included, are counted with the value calculated with the number of UTF-8 bytes. The number of characters cannot be input to fields other than number input fields. Therefore, enter a value while considering the number of UTF-8 bytes if multibyte characters are included.

When an input value includes control characters

Delete control characters when performing registration on each definition screen or outputting a file on the service linkage job or service linkage monitoring job definition screen.

The control characters to be deleted are as follows: 00 to 1F, 7F to 9F, and Unicode control characters (\u200E, \u200F, \u200D, \u200C, \u202A, \u202D, \u202E, \u202C, \u206E, \u206F, \u206B, \u206A, \u206D, \u206C, \u001E, \u001F, \u202B).

Note that 0A (LF) and 09 (tab character) are not deleted from some input items. For those input items where these control characters are not deleted, refer to the input value restrictions of each definition screen.

The available number of characters does not include control characters because, as described above, they are deleted when the number of input characters is counted.

Operation at the time of exporting or importing

When data are exported while being input, the inputs to the screen at the time of export may not be shown on the screen.

Specifically, check the following after importing.

- When the data is exported with only an environment variable name input for the **Environment variables at time of command execution** on the execution definition screen, connection definition screen, and connection definition screen, *environment-variable-name=* is displayed on the screen when the data are imported.
- When the data is exported with only = input for the **Environment variables at time of command execution** on the execution definition screen, connection definition screen, and connection definition screen, a blank line is displayed on the screen when imported.

- When the data are exported and then imported with the **Connection definitions** item selected but no definition selected on the Service linkage job definitions screen or the Service linkage monitoring job definition screen, the item is not selected on the screen.

About the version of the import destination of the exported definition file

Any definition file exported by an upper version must not be imported to a lower version. If you import such a definition file and upgrade JP1/AJS3 for Cloud Service Applications, a problem such as abnormal termination of a linkage job might occur when the definition is used.

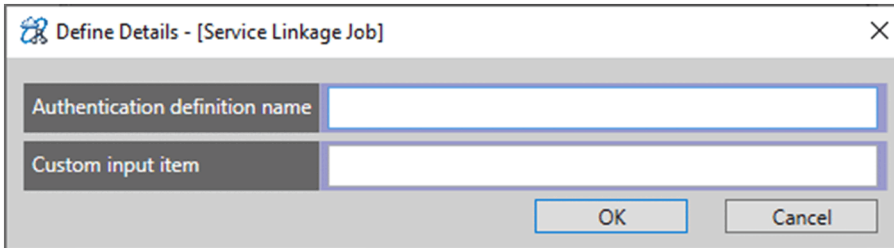
7.2 JP1/AJS3 - View Define Details window

This section describes how to operate the JP1/AJS3 - View Define Details window.

7.2.1 Define Details window for service linkage jobs

The Define Details window for service linkage jobs is explained below.

Figure 7–27: Define Details window for service linkage jobs



The following are display items and restrictions on input values in the Define Details window for **Service Linkage Job**:

Authentication definition name

Enter the authentication definition to be used for the service linkage job.

Custom input item

Enter the custom input item to be used for the service linkage job.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Authentication definition name	Text box	A character string of up to 64 bytes. Alphanumerics, hyphens (-), underscores (_), slashes (/), question marks (?), and periods (.) can be used. Macro variables can be specified for this input item.	Not required	None
2	A value specified in Label Name in AJS3 - View Custom Input Items in the Variable Settings dialog box of the Execution Definition window of the Web GUI	Text box	Restrictions are imposed by the rules specified in Character String Length and Prohibited Characters in AJS3 - View Custom Input Items . For details, see 7.1.8 (4) Setting variables dialog box . Macro variables can be specified for this input item.	Not required	None

7.2.2 Define Details window for service linkage objects monitoring jobs

The Define Details window for service linkage objects monitoring jobs is explained below.

Figure 7–28: Define Details window for service linkage objects monitoring jobs

The screenshot shows a dialog box titled "Define Details - [Service Linkage Objects Monitoring Job]". It has a close button (X) in the top right corner. The dialog contains the following fields and options:

- Authentication definition name:** A text input field.
- Custom input item:** A text input field.
- Name of the object to be monitored:** A text input field.
- Monitoring options:** A section containing three checkboxes: Create, Delete, and Update. To the right of the "Create" checkbox is a dropdown menu with "Establish at objects creation" selected. To the right of the "Delete" checkbox is a dropdown menu with "Holds true when the object is deleted" selected.
- Monitoring interval:** A text input field containing "60" followed by "sec".

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

The following are display items and restrictions on input values in the Define Details window for **Service Linkage Objects Monitoring Job**:

Authentication definition name

Enter the authentication definition to be used for the service linkage objects monitoring job.

Custom input item

Enter the custom input item to be used for the service linkage objects monitoring job.

Name of the object to be monitored

Enter a monitoring target object name, which is one of the object names extracted by the command that acquires object list information. You can specify multiple objects as monitoring targets by specifying a collective name. For details, see [6.2.1 \(4\) About how to specify the names of monitoring target objects](#).

Monitoring options

Specify the condition for monitoring completion from the monitoring target object information.

Create

Monitoring is complete when a monitoring target object is created. An option can be specified to confirm that monitoring is complete if the object is already created during the first monitoring.

Delete

Monitoring is complete when a monitoring target object is deleted. An option can be specified to confirm that monitoring is complete if the object is already deleted during the first monitoring.

Update

Monitoring is complete when a change occurs with the monitoring target object information that is the target of update monitoring. The information to be monitored for updates is the information in **Update monitoring target 1** to **Update monitoring target 3**, which can be specified in **Monitoring processing** in the Object monitoring definition window of the Web GUI.

Monitoring interval

Enter the interval for verifying whether the specified monitoring target object fulfills the condition under which the monitoring condition is met.

No.	Display item	Input format	Input restriction	Required/Not required	Assumed value
1	Authentication definition name	Text box	A character string of up to 64 bytes. Alphanumerics, hyphens (-), underscores (_), slashes (/), question marks (?), and periods (.) can be used. Macro variables can be specified for this input item.	Not required	None
2	Value specified in Label Name in AJS3 - View Custom Input Items in the Variable Settings dialog box of the Object Monitoring Definition window of the Web GUI	Text box	Restrictions are imposed by the rules specified in Character String Length and Prohibited Characters in AJS3 - View Custom Input Items . For details, see 7.1.9 (3) Setting variables dialog box . Macro variables can be specified for this input item.	Not required	None
3	Name of the object to be monitored	Text box	A character string of up to 3,072 bytes. Macro variables can be specified for this input item.	Required	None
4	Option of Create in Monitoring options	List box	Select from below: <ul style="list-style-type: none"> • Establish at objects creation • Establish for existing objects 	Required [#]	Establish at objects creation
5	Option of Delete in Monitoring options	List box	Select from below: <ul style="list-style-type: none"> • Holds true when the object is deleted • Holds true even when it no longer exists 	Required [#]	Holds true when the object is deleted
6	Monitoring interval	Text box	A numerical value between 60 and 600. The unit is seconds.	Required	60

[#]: Specification is required if the applicable monitoring condition is checked. If it is not checked, this item is deactivated.

7.2.3 Notes on Define Details window

This section describes notes on the use of the Define Details window.

About restrictions on entered values

If you enter characters including multibyte characters, the multibyte characters are counted after UTF-8 byte calculation is performed.

If multibyte characters are included, take into consideration the number of UTF-8 bytes before you enter the characters.

In addition, the value entered or selected in the Define Details window will be saved in the subsequent unit definition parameter of JP1/AJS.

- For service linkage jobs: env
- For service linkage monitoring jobs: cprm

For the above-mentioned definition parameters, the maximum total entry size is defined. For this reason, if the value entered in the detailed definition window is within the stipulated range, the KNBB4009-E message might be issued and the definition might fail. In addition, there are values that will automatically be output by the detailed definition window. Therefore, take into consideration the values that will be output by the detailed definition window and make sure that the maximum size will not be exceeded.

For details, see *4.5 Unit definition parameters of service linkage jobs* and *4.6 Unit definition parameters of service linkage monitoring jobs*.

8

Commands

This chapter describes the commands that are used for JP1/AJS3 for Cloud Service Applications.

Command description format

The following describes the command description format, including how to specify commands and the command syntax symbols.

How to specify commands

The commands are specified using the following format:

```
ajsxxx
  [ $\Delta_1$  -option-A [ $\Delta_0$  value-a [, value-b [, value-c ...]]]      ... (1)
  [ $\Delta_1$  -option-B [ $\Delta_0$  value-a [, value-b [, value-c ...]]]      ... (1)
  [ $\Delta_1$  arbitrary-name-X [ $\Delta_1$  arbitrary-name-Y [ $\Delta_1$  arbitrary-name-Z ...]] } ... (2)
```

Legend:

- Δ_0 : Specify zero or more space characters. Spaces can be omitted.
- Δ_1 : Specify one or more space characters. Spaces cannot be omitted.

Here, (1) is called an option, and (2) is called an argument.

The following describes the rules for specifying arguments:

- Specify an option first, and then specify an arbitrary name such as a unit name. If you specify any name before the option, the system assumes the entire specification as a name.
- Multiple options can be specified in any order.
- To specify more than one value for one option, use a comma (,) to separate each value.
- Options without a value can be specified in succession.

Example:

-a-b-c can be specified as -abc.

- Two-byte options without a value cannot be specified in succession.

Example:

-a-ab cannot be specified as -aab, or -cd -cf cannot be specified as -cdcf.

- When specifying options in succession, you can specify a value of the last option.

Example:

In -abc xyz, xyz is a value of the c option.

- If you specify a value for an option that does not have a value, the system assumes anything that follows the value to be a name.
- An error occurs if you specify an invalid option.
- To specify a character string beginning with a hyphen (-) for the first name, such as *arbitrary-name-X* in the above example of command specification, specify -- Δ_1 before *arbitrary-name-X*. (The system assumes anything that follows -- Δ_1 to be a name.)

You do not need to specify -- Δ_1 for the second and subsequent names.

Example:

To specify two names -jobA and -jobB, specify -- -jobA -jobB.

- You can use regular expressions for names.

- An error occurs if the number of specified names exceeds the limit.
- Character strings specified in arguments are case-sensitive. Be careful to use a correct combination of uppercase and lowercase letters.

Symbols used for command syntax explanations

The following table lists the conventions used in command syntax explanations:

Table 8–1: Symbols used for command syntax explanations

Symbol	Convention and example
	Only one of the options separated by a vertical bar can be used at one time. Example: A B C A, B, or C
{ }	One of the items enclosed in braces and separated by a vertical bar must be specified. Example: { A B C } Specify A, B, or C.
[]	The item or items enclosed in brackets are optional. When multiple items are listed, choose one or omit all. Example: [A] Specify A or nothing. [B C] Specify B, C, or nothing.
...	The item or items preceding the ellipsis (. . .) can be repeated. Example: A, B, . . . After A, specify B as many times as necessary.
<u> </u> (underline)	The underlined characters are the system default when you omit all the items enclosed in brackets. If there is no default, only the specified item will take effect. Example: [<u>A</u> B] A is assumed if you do not specify either item.

List of commands

The following table shows the commands for JP1/AJS3 for Cloud Service Applications.

Table 8–2: List of JP1/AJS3 for Cloud Service Applications commands

Functionality	Command name	Windows	Linux	Required privileges	Supported products
Setup the JP1/AJS3 for Cloud Service Applications server.	ajscsasetup	Y	Y	Windows: Administrators Linux: Superuser	C
Start the service of the JP1/AJS3 for Cloud Service Applications.	ajjs_csa	--	Y	Linux: Superuser	C
Stop the service of the JP1/AJS3 for Cloud Service Applications.	ajjs_csa_stop	--	Y	Linux: Superuser	C
Collects the necessary data when a failure occurs.	ajjs_log	--	Y	Linux: Superuser	C
	ajjs_log.bat	Y	--	Windows: Administrators	C
Register the service linkage job or service linkage monitoring job.	ajscsajobreg	Y	--	None	V
List the registered service linkage jobs or service linkage monitoring jobs.	ajscsajoblist	Y	--	None	V
Delete the service linkage job or service linkage monitoring job.	ajscsajobdel	Y	--	None	V

Legend:

Y: Supported

--: Not supported

V: JP1/AJS3 - View

C: JP1/AJS3 for Cloud Service Applications

ajscsasetup (Windows, Linux)

Format

```
ajscsasetup
  -c|-p|-d Shared-directory-name -h Logical-host-name-of-JP1/Base [-m
|-s]
```

Description

Setup the JP1/AJS3 for Cloud Service Applications server.

Execution privileges

In Windows: Administrators privileges

In Linux: Superuser privileges

Storage directory

In Windows:

JP1/AJS3 for Cloud Service Applications-installation-folder\bin\

In Linux:

/opt/jp1ajs3csa/bin/

Arguments

-c

This option displays the setup details of the JP1/AJS3 for Cloud Service Applications server. The following shows the display items and their descriptions.

No.	Display item	Description
1	Logical host name of JP1/Base	When a logical host is set up, this item shows the logical host name.
2	Shared directory name	When a shared directory is used, this item shows the path to the shared directory.

-p

This option returns the configuration of the JP1/AJS3 for Cloud Service Applications server from the cluster configuration to the default one.

The settings of each configuration file are returned to the defaults, including path and log output destination.

-d *Shared-directory-name*

When setting up the JP1/AJS3 for Cloud Service Applications server with a cluster configuration, specify the full path to the shared directory.

The number of characters that can be specified is 2 to 100 (unit: byte).

For Windows, if the first two bytes are specified with characters other than the drive letter (e.g., C:), the command terminates abnormally.

Do not specify a disk on the network drive. Also, do not specify a path including multibyte characters.

Do not specify the drive and the root directory.

As the shared directory, *specified-shared-directory-name*\jps1ajs3csa is created for Windows, and *specified-shared-directory-name*/jps1ajs3csa for Linux. Under this directory, an environment definition file is created, where the database file is copied. This environment definition file is necessary for operating the JP1/AJS3 for Cloud Service Applications server with a cluster configuration. Note that if these directories already exist with the `-m` option specified, the command terminates abnormally. When the `-m` option is specified, make sure that these directories do not exist before executing a command.

-h Logical-host-name-of-JP1/Base

Specify the logical host name where the JP1 user authentication information is set, which is used for cluster configuration.

The number of characters that can be specified is 1 to 255 (unit: byte).

-m

Specify this option when setting up the JP1/AJS3 for Cloud Service Applications server as the primary node of the cluster configuration.

Specify this option together with the `-d` option. If the directory specified for the `-d` option does not exist, the command terminates abnormally.

When setting up the primary node, make sure that the shared disk is mounted.

-s

Specify this option when setting up the JP1/AJS3 for Cloud Service Applications server as the secondary node of the cluster configuration.

Specify this option together with the `-d` option.

When setting up the secondary node, specify the `-d` option with the path to the shared directory that has been specified for setting up the primary node.

Notes

- The information set by the `ajscsasetup` command is reflected the next time the JP1/AJS3 CSA HTTP Server service or the JP1/AJS3 CSA Web Application Server service is started. Therefore, if the setting is changed by the `ajscsasetup` command when the service is in operation, the setting information displayed using `-c` differs from the current operation status.
- When a command is executed with `-c` specified, even if the `ajscsasetup.conf` and `ajs3csaweb.conf` files are invalid, the processing is continued.
- Logs output by this command are always output to a physical host in a cluster configuration environment. In the case of `ajs3csaweb.conf`, this command also always refers to `ajs3csaweb.conf` on the physical host.
- When the `ajscsasetup` command is executed, settings of the user property file for J2EE server (`usrconf.properties`)# might return to the initial state, and startup of JP1/AJS3 CSA Web Application Server services might fail. After the execution of the `ajscsasetup` command, set again the user property file for J2EE server (`usrconf.properties`).

This problem occurs when both of the following conditions are met:

1. The settings of the user property file for J2EE server (`usrconf.properties`) are changed before the execution of the `ajscsasetup` command.
2. The `-d` or `-p` option is specified for the argument of the `ajscsasetup` command.

#:

For details about setup items of the user property file for J2EE server (`usrconf.properties`) to be used for setting the JP1/AJS3 for CSA Web Application Server, see [3.4.3 User property file for J2EE server \(`usrconf.properties`\)](#).

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

Display the setup details of the JP1/AJS3 for Cloud Service Applications server.

```
ajscsasetup -c
```

Output example

```
KNBB2520-I Output of settings data will now start.
Logical host name      logicalhost
Shared directory      E:\share
KNBB2521-I Output of settings data ended.
```

Example 2

This option returns the configuration of JP1/AJS3 for Cloud Service Applications server from the cluster configuration to the default.

```
ajscsasetup -p
```

Example 3

Set up the JP1/AJS3 for Cloud Service Applications server as the primary node when the shared directory is `E:\SHARE` and the logical host of JP1/Base is `logicalhost`.

```
ajscsasetup -d E:\SHARE -h logicalhost
```

or

```
ajscsasetup -d E:\SHARE -h logicalhost -m
```

Example 4

Set up the JP1/AJS3 for Cloud Service Applications server as the secondary node when the shared directory is `E:\SHARE` and the logical host of JP1/Base is `logicalhost`.

```
ajscsasetup -d E:\SHARE -h logicalhost -s
```


jajs_csa (Linux only)

Format

```
jajs_csa  
  [-t {http|app}]
```

Description

Start the service of the JP1/AJS3 for Cloud Service Applications.

Execution privileges

Superuser privilege

Storage directory

/etc/opt/jp1ajs3csa/

Arguments

-t {http|app}

Specify and start a service of JP1/AJS3 for Cloud Service Applications.

http

Start the JP1/AJS3 CSA HTTP Server service.

app

Start the JP1/AJS3 CSA Web Application Server service.

If you omit this option, the JP1/AJS3 CSA Web Application Server service and the JP1/AJS3 CSA HTTP Server service start in that order.

Notes

- This command applies only to Linux. You cannot use this command in Windows.
- If an attempt to start the JP1/AJS3 CSA Web Application Server service fails, stop processing of this service might be performed within the command, causing the KNBB2524-E message to be displayed together with the KNBB2525-E message. In this case, no action is required for the KNBB2525-E message.
- If you execute this command with this option omitted, startup processing is performed for the JP1/AJS3 CSA Web Application Server, and then for the JP1/AJS3 CSA HTTP Server. If an error occurs in the JP1/AJS3 CSA HTTP Server service during startup, the JP1/AJS3 CSA Web Application Server service is still running. The following table lists the services in which an error has occurred and the status of each service.

Table 8–3: Services in which an error occurred and the service status

Service status	Service in which an error has occurred	
	JP1/AJS3 CSA Web Application Server	JP1/AJS3 CSA HTTP Server
Status of JP1/AJS3 CSA Web Application Server	Stop	Running
Status of JP1/AJS3 CSA HTTP Server	Stop	Stop

- If an attempt is made to start the JP1 /AJS3 CSA HTTP Server service while it is already running, the KNBB2524-E message is displayed, and the command terminates abnormally.
- By default, the JP1/AJS3 CSA HTTP Server service is started by the user privilege with the user ID `nobody` and the group ownership `root`. If an attempt to start the service fails with the KNBB2524-E message displayed, check if the `nobody` user exists in the system. If the `nobody` user does not exist, create that user, or open the setting file `/opt/jp1ajs3csa/uCPSB/httpsd/conf/httpsd.conf` in a text editor and specify that user and group ownership for the `User` and `Group` lines.

```
User nobody
Group root
```

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

Start a service of JP1/AJS3 for Cloud Service Applications.

```
jajs_csa
```

Example 2

Start only the JP1/AJS3 CSA HTTP Server service among the services of JP1/AJS3 for Cloud Service Applications.

```
jajs_csa -t http
```

Example 3

Start only the JP1/AJS3 CSA Web Application Server service among the services of JP1/AJS3 for Cloud Service Applications.

```
jajs_csa -t app
```

jajs_csa_stop (Linux only)

Format

```
jajs_csa_stop  
  [-t {http|app}]
```

Description

Stop the service of the JP1/AJS3 for Cloud Service Applications.

Execution privileges

Superuser privilege

Storage directory

/etc/opt/jp1ajs3csa/

Arguments

-t {http|app}

Specify and stop a service of JP1/AJS3 for Cloud Service Applications.

http

Stop the JP1/AJS3 CSA HTTP Server service.

app

Stop the JP1/AJS3 CSA Web Application Server service.

If you omit this option, the JP1/AJS3 CSA HTTP Server service and the JP1/AJS3 CSA Web Application Server service stop in that order.

Notes

- This command applies only to Linux. You cannot use this command in Windows.
- In the case where the JP1/AJS3 CSA HTTP Server service was forcibly terminated last time because, for example, power was turned off, if you use this command to stop the JP1/AJS3 CSA HTTP Server service before restarting it, the KNBB2525-E message is displayed, and the command terminates abnormally.
- When the JP1/AJS3 CSA Web Application Server service stops, the command might terminate with the KNBB2715-W message displayed even though no error message or warning message was output. In such a case, no action is required for the KNBB2715-W message. This situation occurs because some processes have already been stopped internally, and the message indicates that stop processing of the JP1/AJS3 CSA Web Application Server service has completed normally.

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

Stop the JP1/AJS3 for Cloud Service Applications service.

```
jajs_csa_stop
```

Example 2

Stop only the JP1/AJS3 CSA HTTP Server service among the services of JP1/AJS3 for Cloud Service Applications.

```
jajs_csa_stop -t http
```

Example 3

Stop only the JP1/AJS3 CSA Web Application Server service among the services of JP1/AJS3 for Cloud Service Applications.

```
jajs_csa_stop -t app
```

jajs_log (Linux only)

Format

```
jajs_log
  [-h logical-host-name]
  [-f storage-directory]
  [-s]
  [-t]
  [-u]
  [-b]
  [additional-file]
```

Description

This command collects maintenance information, such as the JP1/AJS3 for Cloud Service Applications definitions, operating information, and information about the OS.

By default, the results of executing the data collection tool are output to the following files under `/tmp/jplajs2/trouble/`.

For physical host

1. `JP1_DEFAULT_1st.tar.Z`
The data for the first reports are output.
2. `JP1_DEFAULT_2nd.tar.Z`
The data for the second reports are output.
3. `JP1_DEFAULT_3rd.tar.Z`
All the other data are output.

For logical host

1. `logical-host-name_1st.tar.Z`
The data for the first report are output.
2. `logical-host-name_2nd.tar.Z`
The data for the second report are output.
3. `logical-host-name_3rd.tar.Z`
All the other data are output.

Execution privileges

Superuser privilege

Storage directory

`/opt/jplajs3csa/tools/`

Arguments

-h *logical-host-name*

Specify the name of the target logical host. Data of JP1/Base is collected from the specified logical host.

In addition, the data collection tool collects the data on the physical host in addition to the data on the specified logical host.

If you do not specify a name, the physical host logs are collected.

-f storage-directory

Use a full path without space characters to specify the directory used to store the collected information. If the specified directory name contains a space character, the system assumes that the character string before the space is the storage directory name and treats the characters after the space as other arguments.

When you use a relative path to specify a storage directory, the specified path is created under the root directory and the collected data are stored there.

If you specify a directory that does not exist, a new directory with that name is created. If data have already been collected in the specified storage directory, a message asking whether you want to overwrite the data appears.

If you omit this option, the collected data are output to `/tmp/jp1ajs2/trouble/`.

-s

Specify this option if you do not want to collect information about the database used by JP1/AJS3.

If you do not specify this option, the data collection tool collects information about the database.

-t

Specify this option if you do not want to obtain the `hosts`, `services`, and `password` files.

-u

Specify this option if you do not want to obtain the core file.

Although you specify this option, the back trace information is collected.

-b

Specify this option if you do not want to collect detailed information about JP1/Base.

The detailed information about JP1/Base is the data for the second report, which is output to the `JP1BASE_INFO` directory.

If you do not specify this option, the data collection tool collects detailed information about JP1/Base.

When this option is not specified, it is automatically determined whether to collect the information. Therefore, do not specify this option if you are unsure about whether detailed information about JP1/Base needs to be collected.

Specify this option only when you want to suppress the collection of detailed information about JP1/Base.

If free disk space at the output destination is insufficient, execute the data collection tool with the `-b` option specified, and then execute the data collection tool for JP1/Base (`jobs_log`) to collect detailed information about JP1/Base. For details about the data collection tool for JP1/Base (`jobs_log`), see the *JP1/Base User's Guide*.

additional-file

Use the full path without space characters to specify the file that is not usually obtained by using the data collection tool, such as the core file of the JP1/AJS3 commands. If the specified file name contains a space character, the system assumes that the character string before the space is an additional file name and treats the characters after the space

as other arguments. Using this argument, you can collect information that is not automatically collected by the data collection tool.

If the core file is specified as an additional file, the core file is collected even if you specify the `-u` option.

You can specify a directory name for `additional-file`. If you specify a directory, all the data in the specified directory are collected.

Notes

- If you collect data about a logical host in a cluster configuration, you must mount the shared disk for the logical host.
- The data collection tool uses the `gzip` command to compress the collected data. If the `gzip` command is not installed in the environment where the data collection tool is executed, the data collection tool uses the `tar` command to compress and output the data. It does not use the `compress` command. If the `tar` command is not installed, the data collection tool terminates abnormally, and processing ends.
- Because the user might not have reference permission for a file contained in the script, the superuser must execute the script.
- If you have already created a file containing the results of executing the script, JP1/AJS3 outputs a message asking for permission to overwrite the file. Enter `y` to overwrite the file. If you do not want to overwrite the file, enter `n`.
- If no core dump file is output, a message (`tar: core? Is unknown.The file is not dumped.`) is displayed. This is not a problem.
- If the target product is not installed or is being used by another process, or a file that cannot be accessed because of its file attribute is detected, a message stating that there is no applicable directory or file or that the target file cannot be accessed might be displayed during the collection of data. This is not a problem.
- Because the `ajs2collectcore` command is executed internally while the data collection tool is being executed, some data cannot be collected, depending on the OS. For details, see *ajs2collectcore (UNIX only)* in *3. Commands Used for Normal Operations* in the manual *JP1/Automatic Job Management System 3 Command Reference*.
- If there are no data to be collected, a file containing the execution result of the data collection tool is not created.
- Do not execute more than one data collection tool at the same time.
- The data collection tool executed by an AJS administrator cannot collect information that requires superuser privileges. We recommend that a user with superuser privileges executes the data collection tool.
For an AJS administrator to execute the data collection tool, the following operations must be performed.
 - The output destination file must be deleted before the data collection tool is executed.
 - The JP1 administrator group must be granted write permissions for the output destination directory.
 - The JP1 administrator group must be granted access permissions for the root directory.
 - To specify the additionally collected data, the JP1 administrator group must be granted access permissions.
- When you specify options, do not specify characters or symbols that have special meanings in the script. If you specify such characters and symbols, an unexpected error might occur.
- When the `ajscsasetup` command was used with the `-d` option specified for system setup, you need to manually obtain the directory specified for the `-d` option.

Return values

0	Normal end
Value other than 0	Abnormal end

Messages

Message	Description	System action
Directory <i>directory-name</i> is created	A directory is created.	Continues processing.
Some data could not be collected by AJS Administrator.	Some data could not be collected because an AJS administrator executed the data collection tool.	Continues processing.
Overwrite file (<i>file-name</i>) ok?	This message asks you whether you want to overwrite <i>file-name</i> . Press <i>y</i> to continue the processing, or press <i>n</i> to cancel the processing.	Waits for a user response.
[CAUTION] When a target program is not installed, or when file access fails because some other process is using the file or because a necessary file-access permission is lacking, a message might be output that states that file access failed or a directory or file does not exist. Such a message does not indicate a problem.	This message is displayed when the specified file is being used or was not found during data collection. However, there is no problem.	Continues processing.
Output file name : (<i>file-name</i>)	The file indicated by <i>file-name</i> has been created.	Terminates the processing.
Write permission error (<i>directory-name</i>)	You do not have write permission. Possible reasons are as follows: <ul style="list-style-type: none"> You do not have permission to create a directory. The directory is being used by another process. Correct the error, and then re-execute the data collection tool.	Terminates the processing.
Make directory (<i>directory-name</i>) is unsuccessful	The directory could not be created. Possible reasons are as follows: <ul style="list-style-type: none"> You do not have permission to create a directory. The directory is being used by another process. Correct the error, and then re-execute the data collection tool.	Terminates the processing.
Read permission error (<i>file-name</i>)	You do not have read permission. Obtain read permission, and then re-execute the data collection tool.	Terminates the processing.
File <i>file-name</i> is not found	The directory or file specified as the additional file was not found. Specify a correct path, and then re-execute the data collection tool.	Terminates the processing.
[-s] [-f <i>output-file</i>] [-h <i>Logical-Host-Name</i>] [-t] [-u] [-e] [-b] [<i>add-in-file</i> ...]	The options are specified incorrectly. Specify the options correctly, and then re-execute the data collection tool.	Terminates the processing.
The collection of detailed information on JP1/Base begins.	Collection of detailed information about JP1/Base has started.	Continues processing.

Message	Description	System action
The collection of detailed information on JP1/Base ended.	Collection of detailed information about JP1/Base has ended	Continues processing.

Example 1

The following command collects data about a physical host.

```
jajs_log
```

Example 2

The following command collects data about a logical host (`cluster`).

```
jajs_log -h cluster
```

Example 3

The following command outputs information, including the core file (`/tmp/core`), to a specified file (`/tmp/trouble`).

```
jajs_log -f /tmp/trouble /tmp/core
```

Data that can be collected

The data collection tool collects the data from JP1/AJS3 for Cloud Service Applications in addition to the data from JP1/AJS3 - Manager. The data additionally collected from JP1/AJS3 for Cloud Service Applications are shown below. For details on data collected from JP1/AJS3 - Manager, see *jajs_log or _04 (UNIX only)* in *3. Commands Used for Normal Operations* in the manual *JP1/Automatic Job Management System 3 Command Reference*.

The data for the first reports (`/tmp/jplajs2/trouble/JP1_DEFAULT_1st.tar.z#1`)

Names of directory or file containing collected data	Description
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED^{#2}</code>	Storage destination of shared directory information
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/conf^{#2}</code>	Storage destination of configuration files
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/database^{#2}</code>	Storage destination of database information
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/database/jplajscsadbdef.dat^{#2}</code>	Definition information output result file
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/database/jplajscsadbexe.dat^{#2}</code>	History information output result file
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/log^{#2}</code>	Storage destination of log files
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/sys^{#2}</code>	Storage destination of system files
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED/tmp^{#2}</code>	Storage destination of temporary files
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/etc/opt/jplajs3csa/conf</code>	Storage destination of configuration files excluding the root certificate
<code>/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/opt/jplajs3csa/sys</code>	Storage destination of system files

Names of directory or file containing collected data	Description
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/srvdata	Storage destination of data of the HTTP server and application server
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/srvdata/snapshot.zip	Data of the HTTP server and application server
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/database	Storage destination of database information
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/database/jplajscsadbdef.dat	Definition information output result file
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/database/jplajscsadbexe.dat	History information output result file
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/log	Storage destination of log files
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/sys	Storage destination of system files
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/var/opt/jplajs3csa/tmp	Storage destination of temporary files
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/snapshotlog.txt	Log file output by the tool that collects data of the HTTP server and application server
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/jplajs3csadbinfo.txt	Database information
/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/_csaras.filelist	File list

#1

When the `-f` option is omitted, data are output here.

#2

/tmp/jplajs2/trouble/JP1AJS3CSA_INFO/SHARED and files and directories under it are collected only when setup is executed by using the `ajscssetup` command with the `-d` option specified and when the directories and files exist.

jajs_log.bat (Windows only)

Format

```
jajs_log.bat
  [-h logical-host-name]
  [-f storage-directory]
  [-s]
  [-t]
  [-u]
  [-b]
```

Description

This command collects maintenance information, such as the JP1/AJS3 for Cloud Service Applications definitions, operating information, and information about the OS.

By default, the results of executing the data collection tool are output to the following files under %TEMP%\jplajs2\backlog.

For physical host

1. JP1_DEFAULT\JP1_DEFAULT_1st
The data for the first reports are output.
2. JP1_DEFAULT\JP1_DEFAULT_2nd
The data for the second reports are output.
3. JP1_DEFAULT\JP1_DEFAULT_3rd
All the other data are output.

For logical host

1. *logical-host-name**logical-host-name*_1st
The data for the first report are output.
2. *logical-host-name**logical-host-name*_2nd
The data for the second report are output.
3. *logical-host-name**logical-host-name*_3rd
All the other data are output.

Execution privileges

Administrators privileges

Storage directory

JP1/AJS3 for Cloud Service Applications-installation-folder\tools\

Arguments

-h *logical-host-name*

Specify the name of the target logical host. Data of JP1/Base is collected from the specified logical host.

In addition, the data collection tool collects the data on the physical host in addition to the data on the specified logical host.

If you do not specify a name, the physical host logs are collected.

-f *storage-directory*

Use the absolute path to the folder to which collected data are output. You can also use a relative path from the location in which the command is executed. However, you cannot specify the root directory.

To specify a path that contains spaces, enclose the entire path in double quotation marks ("").

If you specify a folder that does not exist, a new folder with that name is created.

If data have already been collected in the specified storage folder, a message asking whether you want to overwrite the files is displayed.

If you specify too long a path to the storage folder, data collection might fail. If data collection fails, specify a shorter path, and then retry collection data.

If you omit this option, the collected data are output to %TEMP%\jplajs2\backlog. If you specify this option, the value of this option overrides the storage folder that was changed from the default by customizing the tool.

-s

Specify this option if you do not want to collect information about the database used by JP1/AJS3.

If you do not specify this option, the data collection tool collects information about the database.

-t

Specify this option if you do not want to obtain the `hosts`, `services`, and `password` files.

-u

Specify this option if you do not want to obtain dump files.

-b

Specify this option if you do not want to collect detailed information about JP1/Base.

The detailed information about JP1/Base is the data for the second report, which is output to the `JP1BASE_INFO` directory.

If you do not specify this option, the data collection tool collects detailed information about JP1/Base.

When this option is not specified, it is automatically determined whether to collect the information. Therefore, do not specify this option if you are unsure about whether detailed information about JP1/Base needs to be collected.

Specify this option only when you want to suppress the collection of detailed information about JP1/Base.

If free disk space at the output destination is insufficient, execute the data collection tool with the `-b` option specified, and then execute the data collection tool for JP1/Base (`jbs_log`) to collect detailed information about JP1/Base. For details about the data collection tool for JP1/Base (`jbs_log`), see the *JP1/Base User's Guide*.

additional-file

Use the full path without space characters to specify the file that is not usually obtained by using the data collection tool, such as the core file of the JP1/AJS3 commands. If the specified file name contains a space character, the system assumes that the character string before the space is an additional file name and treats the characters after the space as other arguments. Using this argument, you can collect information that is not automatically collected by the data collection tool.

If the core file is specified as an additional file, the core file is collected even if you specify the `-u` option.

You can specify a directory name for `additional-file`. If you specify a directory, all the data in the specified directory are collected.

Notes

- If you execute the data collection tool without the `-s` option specified during startup of the JP1/AJS3 service, the job might end abnormally. In such a case, JP1/AJS3 does not collect information about the ISAM database.
- To collect data about a logical host in a cluster configuration, execute the data collection tool on the logical host on which the logical host runs.
- The data collection tool does not compress the data if collects. To compress the data, use a data compression tool.
- If you have already created a file containing the results of batch files, JP1/AJS3 outputs a message asking for permission to overwrite the file. To override the file, specify `y`. If you do not want to overwrite the file, specify `n`.
- While a batch file is being executed, JP1/AJS3 might display an error message stating that a sharing violation has occurred for a file in the `JP1/Cloud Service Linkage-installation-folder\sys` folder. This is not a problem.
- If you perform an operation on the collected data, such as moving it or deleting it immediately after the execution of the data collection tool has finished, a message reporting that the process cannot access a file because another process is currently using the file might be displayed. This message is displayed because a process that collects OS information internally is still being executed despite termination of the tool. If this message is displayed, wait a while and then retry the operation.
- If you execute the data collection tool while using Outlook, the following message might be displayed:

```
The program is attempting to access email addresses in Outlook. Is this all right?
```

This message is displayed because of the machine configuration collection program (`msinfo32`) that is executed internally by the data collection tool. This program does not affect the operation of the data collection tool or Outlook. The data collection tool does not collect email addresses. If this message is displayed, click the **No** button.

- When you execute the data collection tool, you must open the Command Prompt window as an administrator. If you are not an administrator, UAC will frequently open a confirmation dialog box while the data collection tool is running. If you turn UAC off, you will not need to open the Command Prompt window as an administrator.
- Do not execute more than one data collection tool at the same time.
- When you specify options, do not specify characters or symbols that have special meanings in the batch file. If you specify such characters and symbols, an unexpected error might occur.
- When the `ajscsasetup` command was used with the `-d` option specified for system setup, you need to manually obtain the directory specified for the `-d` option.

Return values

0	Normal end
Value other than 0	Abnormal end

Messages

Message	Description	Action
Finished. Press any key.	The process ended normally. Press any key.	Wait for a user response.
Failed. Press any key.	The process did not end normally. Press any key. See the output OS messages, remove the cause of the error, and then re-execute the process.	Wait for a user response.
File <i>file-name</i> is exist. Delete to continue? (y/n)	A file created the last time this process was executed exists. Press y to delete the file and continue processing, or press n to stop processing.	Wait for a user response.
Directory <i>directory-name</i> is exist. Delete to continue? (y/n)	A directory created the last time this process was executed exists. Press y to delete the directory and continue processing, or press n to stop processing.	Wait for a user response.
Error exist in option.	An option is specified incorrectly. Specify the option correctly, and then re-execute the process.	Complete the process.
The following logical hosts exist, other than the specified logical host. : <i>logical-host-name</i>	A logical host environment other than the one specified for the -h option exists. If necessary, re-execute the process.	After this message, the following message is output: Finished. Press any key.
The collection of detailed information on JP1/Base begins.	Collection of detailed information about JP1/Base has started.	Continue processing.
The collection of detailed information on JP1/Base ended.	Collection of detailed information about JP1/Base has ended.	Continue processing.
The collection of Event Log in text format begins.	Collection of event log data in text format has started.	Continue processing.
The collection of Event Log in text format ended.	Collection of event log data in text format has ended.	Continue processing.

Example 1

The following command collects data about a physical host.

```
jajs_log.bat
```

Example 2

The following command collects physical host data while the JP1/AJS3 service is running.

```
jajs_log.bat -s
```

Example 3

The following command collects data about a logical host (`cluster`).

```
jajs_log.bat -h cluster
```

Data that can be collected

The data collection tool collects the data about JP1/AJS3 for Cloud Service Applications in addition to the data about JP1/AJS3 - Manager. The data additionally collected from JP1/AJS3 for Cloud Service Applications are shown below. For details on data collected from JP1/AJS3 - Manager, see *jajs_log.bat* or *_04.bat (Windows only)* in *3. Commands Used for Normal Operations* in the manual *JP1/Automatic Job Management System 3 Command Reference*.

The data for the first reports (%TEMP%\jplajs2\backlog\JP1_DEFAULT\JP1_DEFAULT_1st"1)

Name of folder or file containing collected data	Description
\JP1AJS3CSA_INFO\ALLUSERSPROFILE	Storage destination of user data
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\conf	Storage destination of configuration files excluding the root certificate
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\database	Storage destination of database information
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\database\jplajscsadbdef.dat	Database definition file output result file (authentication information excluded)
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\database\jplajscsadbexe.dat	History information output result file of the database
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\log	Storage destination of log files
\JP1AJS3CSA_INFO\ALLUSERSPROFILE\tmp	Storage destination of temporary files
\JP1AJS3CSA_INFO\conf	Storage destination of configuration files excluding the root certificate
\JP1AJS3CSA_INFO\database#2	Storage destination of database information
\JP1AJS3CSA_INFO\database\jplajscsadbdef.dat#2	Definition information output result file
\JP1AJS3CSA_INFO\database\jplajscsadbexe.dat#2	History information output result file
\JP1AJS3CSA_INFO\HNTRLib2	Storage destination of log files
\JP1AJS3CSA_INFO\jplcommon_ajs2	Storage destination of product information files
\JP1AJS3CSA_INFO\jplcommon_ajs3csa	Storage destination of log files
\JP1AJS3CSA_INFO\log#2	Storage destination of log files
\JP1AJS3CSA_INFO\SHARED#3	Storage destination of shared folder information
\JP1AJS3CSA_INFO\SHARED\conf#3	Storage destination of configuration files excluding the root certificate
\JP1AJS3CSA_INFO\SHARED\database#3	Storage destination of database information
\JP1AJS3CSA_INFO\SHARED\database\jplajscsadbdef.dat#3	Definition information output result file
\JP1AJS3CSA_INFO\SHARED\database\jplajscsadbexe.dat#3	History information output result file
\JP1AJS3CSA_INFO\SHARED\log#3	Storage destination of log files
\JP1AJS3CSA_INFO\SHARED\tmp#3	Storage destination of temporary files
\JP1AJS3CSA_INFO\srvdata	Data of the HTTP server and application server
\JP1AJS3CSA_INFO\srvdata\snapshot.zip	Data of the HTTP server and application server

Name of folder or file containing collected data	Description
\JP1AJS3CSA_INFO\sys	Storage destination of system files
\JP1AJS3CSA_INFO\tmp#2	Storage destination of temporary files
\JP1AJS3CSA_INFO\Version\ProductInfo.txt	Product information file
\JP1AJS3CSA_INFO\Version\Version.txt	Product information file
\JP1AJS3CSA_INFO\FILELIST.txt	File list output file
\JP1AJS3CSA_INFO\GETERROR.log	Error log file
\JP1AJS3CSA_INFO\JP1AJS3CSA.DAT	Registry information
\JP1AJS3CSA_INFO\PERMISSIONINFO.TXT	Folder permissions output file

#1

When the `-f` option is omitted, data are output here.

#2

Collection is performed only if the relevant folders and files are deployed in the installation destination folder.

#3

\JP1AJS3CSA_INFO\SHARED and the files and directories under it are collected only when setup is executed by using the `ajscssetup` command with the `-d` option specified and when the directories and files exist.

ajscsajobreg (Windows only)

Format

```
ajscsajobreg
  -d service-linkage-definition-information-file-name or service-linkage
-monitoring-definition-information-file-name
  -n custom-job-name or custom-event-job-name
  [-i icon-file-name]
  [-f]
```

Description

This command registers the service linkage job or the service linkage monitoring job.

Execution privileges

Administrators privileges

Storage directory

JP1/AJS3 - View-installation-folder\bin

Arguments

-d *service-linkage-definition-information-file-name or service-linkage-monitoring-definition-information-file-name*

Specify an absolute or relative path to the service linkage definition information file name or the service linkage monitoring definition information file name.

-n *custom-job-name or custom-event-job-name*

For a service linkage job, specify a custom job name.

For a service linkage monitoring job, specify a custom event job name.

The number of characters that can be specified is 1 to 7 (unit: byte).

Only the following characters can be specified.

- English letters (Case-insensitive)
- Numbers
- - (Hyphen)
- _ (Underscore)

When registering a service linkage job, a specified character string with @ added at the end is treated as the custom job name.

-i *icon-file-name*

Specify an absolute or relative path to the icon file name.

If this option is omitted, the default icon is used.

-f

A service linkage job or a service linkage monitoring job of the same name, if any, is forcibly overwritten and registered.

Notes

None.

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

Register a service linkage job under the following conditions:

- Path to a service linkage job definition file: `d:\temp\sldef01.json`
- Service linkage job name: `awss3UL`
- Path to an icon file: Not specified (The default icon is used)

```
ajscsajobreg -d d:\temp\sldef01.json -n awss3UL
```

When a service linkage job has been successfully registered, the following is displayed.

```
KNBB4501-I The service linkage job has been registered. (awss3UL)
```

Example 2

Forcibly overwrite and register a service linkage job under the following conditions.

- Path to a service linkage job definition file: `d:\temp\sldef02.json`
- Service linkage job name: `azbsDL`
- Path to an icon file: `d:\icon\image01.gif`

```
ajscsajobreg -d d:\temp\sldef02.json -n azbsDL -i d:\icon\image01.gif -f
```

When a service linkage job has been successfully registered, the following is displayed.

```
KNBB4501-I The service linkage job has been registered. (azbsDL)
```

Example 3

Register a service linkage monitoring job under the following conditions.

- Path to a service linkage monitoring job definition information file: `d:\temp\sldef03.json`
- Service linkage monitoring job name: `awsm1`
- Path to an icon file: Not specified (The default icon is used)

```
ajscsajobreg -d d:\temp\sldef03.json -n awsm1
```

When a service linkage monitoring job has been successfully registered, the following is displayed.

```
KNBB4501-I The service linkage monitoring job has been registered. (awsm1)
```

Example 4

Forcibly overwrite and register a service linkage monitoring job under the following conditions.

- Path to a service linkage monitoring job definition information file: d:\temp\slmondef04.json
- Service linkage monitoring job name: azbsMON
- Path to an icon file: d:\icon\image04.gif

```
ajscsajobreg -d d:\temp\sldef04.json -n azbsMON -i d:\icon\image04.gif -f
```

When a service linkage monitoring job has been successfully registered, the following is displayed.

```
KNBB4501-I The service linkage monitoring job has been registered. (azbsMON)
```

ajscsajoblist (Windows only)

Format

```
ajscsajoblist
  [-j|-m|-a]
```

Description

This command lists the registered service linkage jobs and service linkage monitoring jobs.

Job names are displayed in ascending order and in the format as follows:

For service linkage jobs:

```
Job name 1
  Service linkage job definition name 1
  Authentication definition name 1
Job name 2
  Service linkage job definition name 2
  Authentication definition name 2
:
```

For service linkage monitoring jobs:

```
Job name 1
  Service linkage monitoring job definition name 1
  Authentication definition name 1
Job name 2
  Service linkage monitoring job definition name 2
  Authentication definition name 2
:
```

When displaying both jobs:

```
service linkage job
Job name 1
  Service linkage job definition name 1
  Authentication definition name 1
Job name 2
  Service linkage job definition name 2
  Authentication definition name 2
:
service linkage monitoring job
Job name 1
  Service linkage monitoring job definition name 1
  Authentication definition name 1
Job name 2
  Service linkage monitoring job definition name 2
  Authentication definition name 2
:
```

Execution privileges

None.

Storage directory

JP1/AJS3 - View-installation-folder\bin\

Arguments

-j

Displays a list of service linkage jobs.

-m

Displays a list of service linkage monitoring jobs.

-a

Displays a list of service linkage jobs and service linkage monitoring jobs.

If arguments are omitted, this command will behave as though **-j** is specified. Note that these arguments cannot be specified concurrently.

Notes

- In the Service Linkage Job Definition window, select the check box for **Specify the default value of the authentication definition specified in the custom job**. The authentication definition name is output only for the service linkage job in which the definition file output by specifying the default authentication definition name is registered. For details on how to output definition files, see [7. Operation](#).
- In the Service linkage monitoring job definition window, select the check box for **Specify the default values for authentication definitions specified in custom event jobs**. The authentication definition name is output only for the service linkage monitoring job in which the definition file output by specifying the default authentication definition name is registered. For details on how to output definition files, see [7. Operation](#).

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

List the registered service linkage jobs when the service linkage jobs of `awss3UL` and `azbsDL` are registered.

```
ajscsajoblist
```

The output is as follows:

```
awss3UL
  /s101
  /auth01
azbsDL
  /s102
  /auth02
```

Example 2

List the registered service linkage jobs when no service linkage job is registered.

```
ajscsajoblist
```

The output is as follows:

```
KNBB4514-W The service linkage job is not registered.
```

Example 3

List the registered service linkage monitoring jobs when the awsm1 and awsm2 service linkage monitoring jobs are registered.

```
ajscsajoblist -m
```

The output is as follows:

```
awsm1
  /s101
  /auth01
awsm2
  /s102
  /auth02
```

Example 4

List the registered service linkage monitoring jobs when no service linkage monitoring job is registered.

```
ajscsajoblist -m
```

The output is as follows:

```
KNBB4514-W The service linkage monitoring job is not registered.
```

Example 5

List the registered service linkage jobs and service linkage monitoring jobs when the awss3UL and azbsDL service linkage jobs are registered, or the awsm1 and awsm2 service linkage monitoring jobs are registered.

```
ajscsajoblist -a
```

The output is as follows:

```
service linkage job
awss3UL
  /s101
  /auth01
azbsDL
  /s102
```

```
/auth02
service linkage monitoring job
awsm1
  /s101
  /auth01
awsm2
  /s102
  /auth02
```

Example 6

List the registered service linkage jobs and service linkage monitoring jobs when the `awss3UL` and `azbsDL` service linkage jobs are registered, or no service linkage monitoring jobs are registered.

```
ajscsajoblist -a
```

The output is as follows:

```
service linkage job
awss3UL
  /s101
  /auth01
azbsDL
  /s102
  /auth02
service linkage monitoring job
KNBB4514-W The service linkage monitoring job is not registered.
```

Example 7

List the registered service linkage jobs and service linkage monitoring jobs when no service linkage jobs are registered, and no service linkage monitoring jobs are registered.

```
ajscsajoblist -a
```

The output is as follows:

```
service linkage job
KNBB4514-W The service linkage job is not registered.
service linkage monitoring job
KNBB4514-W The service linkage monitoring job is not registered.
```

ajscsajobdel (Windows only)

Format

```
ajscsajobdel
  [-j|-m]
  {-n service-linkage-job-name or service-linkage-monitoring-job-name |
  -a}
```

Description

This command deletes the service linkage job or the service linkage monitoring job.

Execution privileges

Administrators privileges

Storage directory

JP1/AJS3 - View-installation-folder\bin

Arguments

-j

Specify this option to delete the service linkage job. If this option is omitted, this command will behave as though **-j** is specified.

This option cannot be specified with **-m** concurrently.

-m

Specify this option to delete the service linkage monitoring job. If this option is omitted, this command will behave as though **-j** is specified.

This option cannot be specified with **-j** concurrently.

-n *service-linkage-job-name* or *service-linkage-monitoring-job-name*

Specify a service linkage job name or a service linkage monitoring job name you want to delete.

If the **-j** option is specified, this is treated as the job name of the service linkage job. If the **-m** option is specified, this is treated as the job name of the service linkage monitoring job.

The number of characters that can be specified is 1 to 7 (unit: byte).

Only the following characters can be specified.

- English letters (Case insensitive)
- Numbers
- - (Hyphen)
- _ (Underscore)

-a

Delete all jobs specified `-j` option or `-m` option.

If omitted any options, delete all service linkage jobs.

This option cannot be specified together with `-n`.

Notes

None.

Return values

0	Normal end
Value other than 0	Abnormal end

Example 1

Delete the registered service linkage jobs `awss3UL`.

```
ajscsajobdel -n awss3UL
```

When a service linkage job has been successfully deleted, the following is displayed.

```
KNBB4515-I The service linkage job has been deleted. (awss3UL)
```

Example 2

Delete the service linkage job `awss3DL`, which does not exist.

```
ajscsajobdel -n awss3DL
```

The output is as follows:

```
KNBB4517-E The specified service linkage job cannot be deleted because it does not exist. (awss3DL)
```

Example 3

Delete all registered service linkage jobs when the service linkage jobs of `awss3UL` and `awss3DL` are registered.

```
ajscsajobdel -a
```

When the service linkage jobs have been successfully deleted, the following are displayed.

```
KNBB4515-I The service linkage job has been deleted. (awss3UL)  
KNBB4515-I The service linkage job has been deleted. (awss3DL)
```

Example 4

Delete the registered service linkage monitoring job `awsm1`.

```
ajscsajobdel -m -n awsml
```

When the service linkage monitoring job has been successfully deleted, the following is displayed.

```
KNBB4515-I The service linkage monitoring job has been deleted. (awsml)
```

Example 5

Delete the service linkage monitoring job `awsm4`, which does not exist.

```
ajscsajobdel -m -n awsm4
```

The output is as follows:

```
The specified service linkage monitoring job cannot be deleted because it does not exist. (awsm4)
```

Example 6

Delete all registered service linkage monitoring jobs when the service linkage monitoring jobs of `awsm1` and `awsm2` are registered.

```
ajscsajobdel -m -a
```

When the service linkage monitoring job has been successfully deleted, the following is displayed.

```
KNBB4515-I The service linkage monitoring job has been deleted. (awsml)
KNBB4515-I The service linkage monitoring job has been deleted. (awsml2)
```

Example 7

Only delete registered service linkage jobs when the service linkage jobs of `awss3UL` and `awss3DL` are registered, or the service linkage monitoring jobs of `awsm1` and `awsm2` are registered.

```
ajscsajobdel -j -a
```

When the service linkage job has been successfully deleted, the following is displayed.

```
KNBB4515-I The service linkage job has been deleted. (awss3UL)
KNBB4515-I The service linkage job has been deleted. (awss3DL)
```

9

Troubleshooting

This chapter describes the procedures for dealing with problems and the data that must be collected.

9.1 Troubleshooting procedure

If a problem occurs in JP1/AJS3 for Cloud Service Applications, use the following procedure to troubleshoot:

1. Check the status.

Check the status of the problem. If a message is output, read it. For details about why each message is output and how to troubleshoot, see *10. Messages*.

2. Collect data.

You need to collect data to identify the cause of a problem. Collect the necessary data after reading *9.3 Data to be collected when a problem occurs* and *9.4 Collecting data for troubleshooting*.

3. Investigate the problem.

Identify the cause of the problem based on the data you have collected. Either pinpoint where the problem occurred or narrow down the problem range.

9.2 Types of log information and storage locations

The following table shows the log information that is output during JP1/AJS3 for Cloud Service Applications operation.

Table 9–1: List of log information

Target host	Log name	Explanation
JP1/AJS3 for Cloud Service Applications server	System failure log	Logs information about system problems for system administrators. For details, see the description of System failure log in the manual, <i>JP1/Automatic Job Management System 3 Troubleshooting</i> .
	Application server common logs	The system outputs logs when the application server starts and stops. For details, see <i>9.2.1 Application Server Common Logs</i> .
	Application server logs	The system outputs logs of screen operations of JP1/AJS3 for Cloud Service Applications. For details, see <i>9.2.2 Application Server Logs</i> .
	Application server logs (for executing service linkage monitoring jobs)	The system outputs information regarding JP1/AJS3 for Cloud Service Applications requests when a service linkage monitoring job is executed. For details, see <i>9.2.3 Application server logs (for executing service linkage monitoring jobs)</i> .
	Server job logs	The system outputs the service linkage job information or the service linkage monitoring job information, JP1/AJS3 - Agent host information, JP1/AJS3 - Manager host information, and job information, when a service linkage job or service linkage monitoring job is executed. In addition, separate logs are output for each service linkage job and service linkage monitoring job. For details, see <i>9.2.4 Server Job Logs</i> .
	Trace log	Outputs maintenance information. The internal format is not disclosed.
	Command log	The system outputs the log of command operations for JP1/AJS3 for Cloud Service Applications. For details, see <i>9.2.5 Command Log</i> .
<ul style="list-style-type: none"> • JP1/AJS3 - Manager host • JP1/AJS3 - Agent host 	Service linkage job log	The system outputs the operation history of service linkage jobs. For details, see <i>9.2.6 Service Linkage Job Log</i> .
	Service linkage job trace log	Outputs maintenance information regarding service linkage jobs. The internal format is not disclosed.
	Service linkage monitoring job log	The system outputs the operation history of the service linkage monitoring job. For details, see <i>9.2.7 Service Linkage Monitoring Job Log</i> .
	Service linkage monitoring log	Outputs maintenance information regarding service linkage monitoring jobs. The internal format is not disclosed.
JP1/AJS3 - View host	Service linkage job or service linkage monitoring job operation command log	Outputs maintenance information of registration, deletion, and list display commands of service linkage jobs or service linkage monitoring jobs. The internal format is not disclosed.
	Service linkage job or service linkage monitoring job operation command error information log	Outputs maintenance information when an error occurs in the registration, deletion, and list display commands of service linkage jobs or service linkage monitoring jobs. The internal format is not disclosed.

Target host	Log name	Explanation
JP1/AJS3 - View host	Service linkage job or service linkage monitoring job definition log	Outputs maintenance information of detailed definition screen of unit of service linkage jobs or service linkage monitoring jobs. The internal format is not disclosed.

9.2.1 Application Server Common Logs

Outputs logs when the application server starts and stops.

The output format of the application server common log is shown below.

```
OS-informationΔHost-nameΔTime-zoneΔLog-function-start-time
NumberΔDateΔTimeΔProduct-identifierΔProcess-IDΔThread-IDΔMessage-IDΔMessage-
text
:
```

Legend:

Δ: Space character

Details of output items are described below.

OS information

The system outputs information about the operating system on which the log function is running.

Host name

The system outputs the name of the host on which the log function is running.

Time zone

The system outputs the time zone of the operating system.

Log function start time

The system outputs the log function start time.

Number

The system outputs the four-digit serial number of the common log for application servers.

Date and Time

The system outputs the acquisition date and time of the common log for application server.

Product identifier

The system outputs the name identifying the product.

Process ID

Process ID is output as a hexadecimal number.

Thread ID

ID to identify threads is output as a hexadecimal number.

Message ID

The system outputs the Message ID. For details of message, see [10. Messages](#).

Message text

The system outputs the message text corresponding to the Message ID. For details of message, see [10. Messages](#).

An example of the output of the application server common log is shown below:

```
**** Microsoft WindowsNT6.1 (Build:7601) Service Pack 3 host1 TZ=(local)-9:0
0 2022/04/07 11:03:20.713
0001 2022/04/22 11:40:41.763 AJS3forCSA 00001AFC 0000144C KNBB3001-I Sta
rt the startup process of the CSA Web Application Server service
:
```

Cautionary note

When log records in a log file are wrapped around to the next file, the original file is not deleted but is overwritten with new log records from the top of the file. To distinguish between log records output before and after wrapping around, the following character string (endpoint identifier) is output at the end of the latest log record.

```
-----< End of Data >-----
```

The endpoint identifier that is output at the end of the previous log is deleted, and the endpoint identifier is output again after a new log is output. Therefore, note the following points when referencing a job execution history log file:

- To check the latest log data, reference the log data preceding the endpoint identifier. The log data that follows the endpoint identifier is the log records output before wrapping around.
- If the log records in a log file have been wrapped around in special timing, two or more endpoint identifiers might remain in the job execution history log file. In such a case, the first endpoint identifier counted from the top of the file is valid.

9.2.2 Application Server Logs

Outputs logs when the application server starts and stops.

The output format of the application server log is the same as the application server common log. For details, see [9.2.1 Application Server Common Logs](#).

The output format of the application server log is shown below.

```
**** Microsoft WindowsNT6.1 (Build:7601) Service Pack 3 host1 TZ=(local)-9:0
0 2022/04/07 11:03:20.713
0001 2022/04/22 11:40:41.763 AJS3forCSA 00001AFC 0000144C KNBB3212-E The
user name or password is invalid.
:
```

9.2.3 Application server logs (for executing service linkage monitoring jobs)

The system outputs information regarding requests sent to JP1/AJS3 for Cloud Service Applications, when a service linkage monitoring job is executed.

Application server logs (for executing service linkage monitoring jobs) are output in the same format as application server common logs. For details, see [9.2.1 Application Server Common Logs](#).

9.2.4 Server Job Logs

The system outputs the service linkage job information or service linkage monitoring job information, JP1/AJS3 - Agent host information, JP1/AJS3 - Manager host information, and job information, when a service linkage job or service linkage monitoring job is executed. In addition, separate logs are output for each service linkage job and service linkage monitoring job.

The output format of the server job log is the same as the application server common log. For details, see [9.2.1 Application Server Common Logs](#).

The output format of the server job log is shown below.

```
**** Microsoft WindowsNT6.1 (Build:7601) Service Pack 3 host1 TZ=(local)-9:0
0 2022/04/07 11:03:20.713
0001 2022/04/22 11:40:41.763   AJS3forCSA  00001AFC 0000144C KNBB3034-I UUID
ΔJP1 user name for job executionΔAgent-host-nameΔManager-host-nameΔSchedule
r-servicenameΔFull-unit-nameΔExecution-IDΔJob-IDΔService-linkage-job-informa
tion-definition-nameΔAuthentication-definition-nameΔLinked-service-nameΔOver
view of-linked-processingΔCLI-for-execution-processingΔJP1-resource-group-na
me
:
```

Legend:

Δ: Space character

9.2.5 Command Log

The system outputs the log of command operations for JP1/AJS3 for Cloud Service Applications.

The output format of the command log is the same as that of the application server common log. For details, see [9.2.1 Application Server Common Logs](#).

9.2.6 Service Linkage Job Log

When a service linkage job is executed, a service linkage job log is output to the JP1/AJS3 - Manager host or JP1/AJS3 - Agent host.

The output format of service linkage job log is shown below.

```
DateΔTimeΔProcess-IDΔThread-IDΔMessage-IDΔMessage-text
:
```

Legend:

Δ: Space character

Details of output items are described below.

Date and Time

The system outputs date and time of acquisition of the server job log.

Process ID

Process ID is output as a hexadecimal number.

Thread ID

ID to identify threads is output as a hexadecimal number.

Message text

The system outputs the message text shown below.

Table 9–2: Output format of message text for service linkage jobs log

Output
The system outputs the message text with the Message ID in the following format: For details of message, see <i>10. Messages</i> .
<code>Message IDΔMessage text corresponding to the Message ID</code>
The following format is output when jobs are started:
<code>KNBB6000-I Starting service linkage job scheduler-service-name:unit-completion-name:execution-IDΔOS-user-name-when-executing-jobΔman ager-host-nameΔJP1-user-name-when-executing-jobΔjob-IDΔagent-host-name</code>
The value of the environment variable name specified by the unit definition for the service linkage job is output in the following format.
<code>Environment variable name=value</code>
For defining jobs in JP1/AJS3 for Cloud Service Applications, when the log output settings in Trace information settings are specified as Output the executed command line, Output the standard output, and Output the standard error output, then logs will be output in the following format.
<code>KNBB6004-I Processing name Service linkage job executed by the command line. CLI_STDOUT:Standard output for the command executed by the service linkage job# CLI_STDERR:Standard error output for the command executed by the service linkage job#</code>
#: If there is no standard output or standard error output, nothing is output. If there are multiple lines, each line is output in the above format.
When a job is completed, message text that indicates completion is output in the following format.
<code>Job ended. RET=return-value</code>

9.2.7 Service Linkage Monitoring Job Log

When a service linkage monitoring job is executed, a log is output to the JP1/AJS3 - Manager host or JP1/AJS3 - Agent host, based on the type of service linkage monitoring job. The output format of the service linkage monitoring job log is shown below.

```
DateΔTimeΔProcess-IDΔThread-IDΔMessage-IDΔMessage-text  
:
```

Legend:

Δ: Space character

Details of output items are described below.

Date and Time

The system outputs the date and time of acquisition of the service linkage objects monitoring job log.

Process ID

Process ID is output as a hexadecimal number.

Thread ID

ID to identify threads is output as a hexadecimal number.

Message text

The system outputs message text based on the type of monitoring job.

(1) Service linkage objects monitoring job log message text

The output format of the message text for the service linkage objects monitoring job log is shown below.

Table 9–3: Output format of message text for the service linkage objects monitoring job log

Output
<p>The system outputs the message text with the Message ID in the following format: For details of message, see <i>10. Messages</i>.</p> <pre>Message IDΔMessage text corresponding to the Message ID</pre>
<p>The message is output in the following format when a monitoring job starts (including monitoring restart that is accompanied with service restart).</p> <pre>KNBB6005-I The service linkage objects monitoring job will be started. (monitoring-target-file-name)</pre>
<p>Messages are output in the following format when a monitoring job starts (including monitoring restart that is accompanied with service restart), and at each monitoring interval.</p> <pre>Maintenance information 1:WatchStart:UUID cloud-service-linkage-authentication-information-name service-linkage-objects-monitoring-job-definition-name manager-host-name scheduler-service-name execution-ID unit-ID JPI-user-name</pre>
<p>If Output the executed command line, Output the standard output, and Output the standard error output are selected in Log output settings under Trace information settings for the definition in JP1/AJS3 for Cloud Service Applications, messages are output in the following format when the information acquisition command is executed.</p> <pre>KNBB6004-I process-name command-line-executed-by-the-service-linkage-objects-monitoring-job CLI_STDOUT: standard-output-for-the-command-executed-by-the-service-linkage-objects-monitoring-job# CLI_STDERR: standard-error-output-for-the-command-executed-by-the-service-linkage-objects-monitoring-job#</pre> <p>#: If there is no standard output or standard error output, nothing is output. If there are multiple lines, each line is output in the above format.</p>
<p>When a job is completed, message text that indicates completion is output in the following format.</p> <pre>Job ended. RET=return-value</pre>

9.2.8 List of log files and directories

(1) Log files and directories in Windows

The log file names and folder names of the Windows versions of JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager, JP1/AJS3 - Agent, and JP1/AJS3 - View are shown below.

The *Log name* column lists the names of the logs created by JP1/AJS3 for Cloud Service Applications.

In *Log file and folder names* column, the following abbreviations are used for folders:

1. CSA_Path

- If the installation folder is the default installation folder or is in a folder protected by the system^{#1}:
%ALLUSERSPROFILE%#2\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA
- If the installation folder is other than the above:
JP1/AJS3 - for Cloud Service Applications-installation-folder

The default installation folder is *system-drive*\Program Files (x86)\HITACHI\JP1AJS3CSA.

2. Mgr_Path

- If the installation folder is the default installation folder or is in a folder protected by the system^{#1}:
%ALLUSERSPROFILE%#2\Hitachi\JP1\JP1_DEFAULT\JP1AJS2
- If the installation folder is other than the above:
JP1/AJS3 - Manager-installation-folder

The default installation folder is *system-drive*\Program Files (x86)\HITACHI\jp1ajs2.

3. Agt_Path

- If the installation folder is the default installation folder or is in a folder protected by the system^{#1}:
%ALLUSERSPROFILE%#2\Hitachi\JP1\JP1_DEFAULT\JP1AJS2
- If the installation folder is other than the above:
JP1/AJS3 - Agent-installation-folder

The default installation folder is *system-drive*\Program Files (x86)\HITACHI\jp1ajs2.

4. View_Path

%ALLUSERSPROFILE%#2\Hitachi\JP1\JP1_DEFAULT\JP1AJS2V

#1

A *folder protected by the system* is the path to a folder in any of the following:

- *system-drive*\Windows
- *system-drive*\Program Files
- *system-drive*\Program Files (x86)

#2

The default for %ALLUSERSPROFILE% is *system-drive*\ProgramData.

In a cluster system, unless otherwise specified, make the substitutions shown in the following table for the indicated abbreviations.

Table 9–4: Log output folders in a cluster system

Abbreviation in Table 8-4 to Table 8-7	Log output folder in a cluster system
<i>CSA_Path</i>	<i>shared-disk-name</i> \jp1ajs3csa
<i>Mgr_Path</i>	<i>shared-disk-name</i> \jp1ajs2
<i>Agt_Path</i>	<i>shared-disk-name</i> \jp1ajs2

The *Default disk space* column indicates the disk space allocated to a log file when the default environment settings is used for operation, and is the total disk space size when there are multiple log files. If the user has not changed the size of a log file, the disk space indicated in the table is the disk space allocated to that log file.

The *Maximum disk space* column indicates the maximum amount of disk space that a log file uses. This value includes changes to definitions, and is the total disk space size when there are multiple log files. The values in this column are the maximum values for log files whose size varies according to the definitions.

The *Timing for switching files* column indicates either a limit or the point at which JP1/AJS3 for Cloud Service Applications switches the log file (output file for the log) to another file. A value in this column indicates that there are multiple log files, and that the file with the oldest update date is overwritten when the maximum disk space has been reached. The values in parentheses indicate the default timing for switching log files.

Table 9–5: Log files and folders in JP1/AJS3 for Cloud Service Applications (for Windows)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Application server common log	<i>CSA_Path</i> \log\appserver{1 2}.log	16,384	16,384	8,192
Application server log	<i>CSA_Path</i> \log\appserver ^N ^{#3} .log	16,384	262,144	8,192
Application server log (for executing service linkage monitoring jobs)	<i>CSA_Path</i> \log\appservermon ^N ^{#4} .log	16,384	262,144	8,192
Server job log	<i>CSA_Path</i> \log\appserverjob ^N ^{#5} .log	33,792	262,144	11,264
Server job log (for executing service linkage monitoring jobs)	<i>CSA_Path</i> \log\appserverjobmon ^N ^{#6} .log	33,792	262,144	11,264
Trace log ^{#7}	<i>CSA_Path</i> \log\csatrace{1 2}.log	16,384	16,384	8,192
Trace log (for executing service linkage monitoring jobs) ^{#9}	<i>CSA_Path</i> \log\csatracemon{1 2}.log	16,384	16,384	8,192
Command log	<i>CSA_Path</i> \log\CommandName ^{#7} ^N ^{#8} .log	256	262,144	128

#1

The unit is kilobytes unless otherwise specified.

#2

The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.

#3

N is an integer from 1 to the value specified by `SERVER_LOG_APP_NUM` (number of log files of application server) in the environment setting file (`ajs3csaweb.conf`).

#4

N is an integer from 1 to the value specified by `SERVER_LOG_APP_MON_NUM` (number of log files of the application server (for executing service linkage monitoring jobs)) in the environment setting file (`ajs3csaweb.conf`).

#5

N is an integer from 1 to the value specified by `SERVERJOB_LOG_JOB_NUM` (number of log files of server jobs) in the environment setting file (`ajs3csaweb.conf`).

#6

N is an integer from 1 to the value specified by `SERVER_LOG_JOB_MON_NUM` (number of log files of server jobs (for executing service linkage monitoring jobs)) in the environment setting file (`ajs3csaweb.conf`).

#7

The file name begins with the name of the next command that was executed.

- `ajscsasetup`
- `jajs_csa_service`

Note that logs output by using the `ajscsasetup` command are always output by the physical host, even in a cluster configuration environment. In addition, the format is not disclosed for the information output for logs related to `jajs_csa_service`.

#8

N is an integer from 1 to the value specified by `COM_LOG_NUM` (number of log files of commands) in the environment setting file (`ajs3csaweb.conf`).

#9

The format of the information output is not disclosed.

Table 9–6: Log files and folders in JP1/AJS3 - Manager (for Windows)

Log name	Log file and folder names	Default disk space#1	Maximum disk space#1	Timing for switching files#2
Service linkage job log	<i>Mgr_Path</i> \log\ajscs aexec{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage job trace log#3	<i>Mgr_Path</i> \log\ajscs atrace	20,480	20,480	Wraparound
Service linkage objects monitoring job log	<i>Mgr_Path</i> \log\ajscs aobjwatch{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage objects monitoring log#3	<i>Mgr_Path</i> \log\ajscs aobjmond	26,624	26,624	Wraparound

#1

The unit is kilobytes unless otherwise specified.

#2

The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.

#3

The format of the output information is not disclosed.

Table 9–7: Log files and folders in JP1/AJS3 - Agent (for Windows)

Log name	Log file and folder names	Default disk space#1	Maximum disk space#1	Timing for switching files#2
Service linkage job log	<i>Agt_Path</i> \log\ajscsa exec{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage job trace log#3	<i>Agt_Path</i> \log\ajscsa trace	20,480	20,480	Wraparound
Service linkage objects monitoring job log	<i>Agt_Path</i> \log\ajscsa objwatch{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Service linkage objects monitoring log ^{#3}	<i>Agt_Path</i> \log\ajscsaobjmond	26,624	26,624	Wraparound

- #1
The unit is kilobytes unless otherwise specified.
- #2
The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.
- #3
The format of the information output is not disclosed.

Table 9–8: Log files and folders in JP1/AJS3 - View (for Window)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Service linkage job or service linkage monitoring job operation command log ^{#3}	<i>View_Path</i> \log\csajobreg[#nnnn_]#4{1 2}.log	2,048	2,048	1,024
Service linkage job or service linkage monitoring job operation command error information log ^{#3}	<i>View_Path</i> \log\ajscsaajobreg{1 2}.log	2,048	2,048	1,024
Service linkage job definition log	<i>View_Path</i> \log\csadefcustom_jobname ^{#5} {1 2}.log	100	100 ^{#5}	50
Service linkage monitoring job definition log	<i>View_Path</i> \log\csadefmoncustom_event_jobname ^{#6} {1 2}.log	100	100 ^{#6}	50

- #1
The unit is kilobytes unless otherwise specified.
- #2
The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.
- #3
The format of the information output is not disclosed.
- #4
Assigns any value between 0001 and 9999 to *nnnn* in *#nnnn_* and creates the log file.
- #5
Create according to the number of registered service linkage jobs (custom jobs). Therefore, the maximum disk usage will increase or decrease depending on the number of registered service linkage jobs.
- #6
Create according to the number of registered service linkage monitoring jobs (custom event jobs). Therefore, the maximum disk usage will increase or decrease depending on the number of registered service linkage monitoring jobs.

(2) Log files and directories in Linux

The log file names and folder names of the Linux versions of JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager, JP1/AJS3 - Agent, and JP1/AJS3 - View are shown below.

The *Log name* column lists the names of the logs created by JP1/AJS3 for Cloud Service Applications.

In *Log file and folder names* column, the following abbreviations are used for folders:

In a cluster system, consider the path names indicate the directories in the Log output directory in a cluster system column in the following table unless otherwise specified.

Table 9–9: Log output directories in a cluster system

Value in Table 8-9 and Table 8-11	Log output folder in a cluster system
/var/opt/jplajs2/	shared-disk-name/jplajs2
/var/opt/jplajs3csa/	shared-disk-name/jplajs3csa

The *Default disk space* column indicates the disk space allocated to a log file when the default environment settings is used for operation, and is the total disk space size when there are multiple log files. If the user has not changed the size of a log file, the disk space indicated in the table is the disk space allocated to that log file.

The *Maximum disk space* column indicates the maximum amount of disk space that a log file uses. This value includes changes to definitions, and is the total disk space size when there are multiple log files. The values in this column are the maximum values for log files whose size varies according to the definitions.

The *Timing for switching files* column indicates either a limit or the point at which JP1/AJS3 for Cloud Service Applications switches the log file (output file for the log) to another file. A value in this column indicates that there are multiple log files, and that the file with the oldest update date is overwritten when the maximum disk space has been reached. The values in parentheses indicate the default timing for switching log files.

Table 9–10: Log files and folders in JP1/AJS3 for Cloud Service Applications (Linux)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Application server common log	/var/opt/jplajs3csa/log/appserversys{1 2}.log	16,384	16,384	8,192
Application server log	/var/opt/jplajs3csa/log/appserverN ^{#3} .log	16,384	262,144	8,192
Application server log (for executing service linkage monitoring jobs)	/var/opt/jplajs3csa/log/appservermonN ^{#4} .log	16,384	262,144	8,192
Server job log	/var/opt/jplajs3csa/log/appserverjobN ^{#5} .log	33,792	262,144	11,264
Server job log (for executing service linkage monitoring jobs)	/var/opt/jplajs3csa/log/appserverjobmonN ^{#6} .log	33,792	262,144	11,264
Trace log ^{#9}	/var/opt/jplajs3csa/log/csatrace{1 2}.log	16,384	16,384	8,192
Trace log (for executing service linkage monitoring jobs) ^{#9}	/var/opt/jplajs3csa/log/csatracemon{1 2}.log	16,384	16,384	8,192

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Command log	/var/opt/ jp1ajs3csa/log/ CommandName ^{#7} N ^{#8} .log	256	262,144	128

#1

The unit is kilobytes unless otherwise specified. The value in parentheses is the kilobyte value expressed in gigabytes.

#2

The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.

#3

N is an integer from 1 to the value specified by SERVER_LOG_APP_NUM (number of log files of application server) in the environment setting file (ajs3csaweb.conf).

#4

N is an integer from 1 to the value specified by SERVER_LOG_APP_MON_NUM (number of log files of the application server (for executing service linkage monitoring jobs)) in the environment setting file (ajs3csaweb.conf).

#5

N is an integer from 1 to the value specified by SERVERJOB_LOG_JOB_NUM (number of log files of server jobs) in the environment setting file (ajs3csaweb.conf).

#6

N is an integer from 1 to the value specified by SERVER_LOG_JOB_MON_NUM (number of log files of server jobs (for executing service linkage monitoring jobs)) in the environment setting file (ajs3csaweb.conf).

#7

The file name begins with the name of the next command that was executed.

- ajscsasetup
- jajs_csa
- jajs_csa_stop

Note that logs output by using the ajscsasetup command are always output by the physical host, even in a cluster configuration environment.

#8

N is an integer from 1 to the value specified by COM_LOG_NUM (number of log files of commands) in the environment setting file (ajs3csaweb.conf).

#9

The format of the information output is not disclosed.

Table 9–11: Log files and folders in JP1/AJS3 - Manager (for Linux)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Service linkage job log	/var/opt/ jp1ajs2/log/ ajscsaexec{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage job trace log ^{#3}	/var/opt/ jp1ajs2/log/ ajscsatrace	20,480	20,480	Wraparound
Service linkage objects monitoring job log	/var/opt/ jp1ajs2/log/ ajscsaobjwatch{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Service linkage objects monitoring log ^{#3}	/var/opt/jplajs2/log/ajscsaobjmond	26,624	26,624	Wraparound

#1
The unit is kilobytes unless otherwise specified. The value in parentheses is the kilobyte value expressed in gigabytes.

#2
The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.

#3
The format of the information output is not disclosed.

Table 9–12: Log files and folders in JP1/AJS3 - Agent (for Linux)

Log name	Log file and folder names	Default disk space ^{#1}	Maximum disk space ^{#1}	Timing for switching files ^{#2}
Service linkage job log	/var/opt/jplajs2/log/ajscsaexec{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage job trace log ^{#3}	/var/opt/jplajs2/log/ajscsatrace	20,480	20,480	Wraparound
Service linkage objects monitoring job log	/var/opt/jplajs2/log/ajscsaobjwatch{01 02 03 04 05 06 07 08 09 10}.log	256,000	1,126,400	Log file size of environment setting parameter (25,600)
Service linkage objects monitoring log ^{#3}	/var/opt/jplajs2/log/ajscsaobjmond	26,624	26,624	Wraparound

#1
The unit is kilobytes unless otherwise specified. The value in parentheses is the kilobyte value expressed in gigabytes.

#2
The value in parentheses in this column indicates the default timing for switching log files. The unit is kilobytes.

#3
The format of the information output is not disclosed.

9.3 Data to be collected when a problem occurs

This section describes the data you need to collect when a problem occurs in JP1/AJS3 for Cloud Service Applications.

JP1 provides data collection tools for batch collection of required data. Data that can be collected using the initial settings of the data collection tools are indicated with symbols in the tables above.

9.3.1 Data to collect

(1) Log information about the OS

You need to collect the following log information about the OS.

(a) Data to collect in Windows

Table 9–13: OS log information that must be collected when a problem occurs (for Windows)

Type of information	Default storage location for files	Collection by the tool
Windows event log	Event log file	Y
Windows registry information	--	Y
hosts file services file	<ul style="list-style-type: none"><i>system-folder</i>\system32\drivers\etc\hosts<i>system-folder</i>\system32\drivers\etc\services	Y
Machine configuration ^{#1}	--	Y
List of program products with running services ^{#1}	--	Y
Network configuration ^{#1}	--	Y
Memory dump ^{#2}	--	N
Crash dump ^{#2}	--	N
Problem report	--	N

Legend:

Y: The data collection tools can collect data.

N: The data collection tools cannot collect data.

#1

Various kinds of computer information that include this information, such as the hardware environment, software environment, and Internet environment, can be obtained. Obtaining this information might take several minutes. Wait until the System Information dialog box closes.

#2

Windows memory dumps and crash dumps cannot be acquired with the data collection tool. Collect the corresponding information manually when a problem occurs.

For the collection method, see [9.4.1\(1\)\(c\) Obtain a dump file](#) and [9.4.1\(1\)\(d\) Collect problem reports](#).

(b) Data to collect in Linux

Table 9–14: OS log information that must be collected when a problem occurs (for Linux)

Type of information	Default storage location for files	Collection by the tool
syslog	/var/log/messages*	Y
hosts file services file passwd file inittab file	/etc/hosts /etc/services /etc/passwd /etc/inittab	Y
Patch information for each OS	--	Y
Shared library file for each OS	--	Y
List of processes	--	Y
core file	--	N
Network information	--	Y
Information about installed Hitachi products	/etc/.hitachi/pplistd/pplistd	Y

Legend:

Y: The data collection tools can collect data.

N: The data collection tools cannot collect data.

(2) Information about JP1

You need to collect the following information about JP1. If the problem occurs while your system is connected to a network, you also need to obtain the files on the JP1/AJS3 - Manager host to which the system is connected.

(a) Data to collect in Windows

Table 9–15: JP1 information to be collected for a problem occurring (for Windows)

Type of information	Default storage location for files	Collection by the tool
Log files	It depends on where JP1/AJS3 for Cloud Service Applications are installed. When JP1/AJS3 for Cloud Service Applications is installed in the default installation location, under the <i>system drive</i> \Windows folder, or under the <i>system drive</i> \Program Files folder %ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA\log When JP1/AJS3 for Cloud Service Applications is installed in a folder other than the above <i>JP1/AJS3 - for Cloud Service Applications-installation-folder</i> \log	Y
Settings file	<i>JP1/AJS3 - for Cloud Service Applications-installation-folder</i> \conf	Y
Get folder access rights	<i>JP1/AJS3 - for Cloud Service Applications-installation-folder</i> \	Y
Integrated trace log folder	<i>system drive</i> \Program Files\hitachi\HNTRLib2	Y

Type of information	Default storage location for files	Collection by the tool
Thread dump	<i>JP1/AJS3 - for Cloud Service Applications-installation-folder\uCPSB\CC\server\public\ejb\ajs3csa</i>	Y
Database information	--	Y

Legend:

Y: The data collection tools can collect data.

#

The default for %ALLUSERSPROFILE% is *system-drive\ProgramData*.

(b) Data to collect in Linux

Table 9–16: JP1 information that must be collected when a problem occurs (for Linux)

Type of information	Default storage location for files	Collection by the tool
Log files	<i>/var/opt/jp1ajs3csa/log</i>	Y
Settings file	<i>/opt/jp1ajs3csa/conf</i>	Y
Get folder access rights	<i>/opt/jp1ajs3csa</i>	Y
Integrated trace log folder	<i>/var/opt/hitachi/HNTRLib2/spool</i>	Y
Thread dump	<i>/opt/jp1ajs3csa/uCPSB/CC/server/public/ejb/ajs3csa</i>	Y
Database information	--	Y

Legend:

Y: The data collection tools can collect data.

Important

When you collect information, use the tar command instead of the cp command. Because the directory from which files are obtained also contains system files, using the cp command might lead to unexpected results.

(3) List of processes

(a) Data to collect in Windows

In Windows, start Task Manager and open the **Processes** page. Check the operating status of processes.

For details about JP1/AJS3 processes, see Processes (for Windows) in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

(b) Data to collect in Linux

Use the ps command to check the operating status of processes.

For details about JP1/AJS3 processes, see Processes (for Linux) in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

(4) Operation data

Collect the following information about the operation that was being performed when the problem occurred:

- Details about the operation
- Time that the problem occurred
- Machine configuration (the version of each OS, host name, JP1/AJS3 for Cloud Service Applications and JP1/AJS3 - Manager, JP1/AJS3 - View configuration)
- Whether the problem is reproducible
- Login user name for the Windows host or Linux host using JP1/AJS3 for Cloud Service Applications

(5) Error information displayed on the screen

Make hard copies of the following:

- Windows on the screen when an application error has occurred
- Error message dialog box (and display the displayed information when a details button (if there is one) is clicked)

(6) Other information

In addition to the above information, you need to collect the following information:

- Contents of **System Log** and **Application Log** of the Windows Event Viewer window
- Arguments specified in a command when the problem occurs during the execution of a command

9.4 Collecting data for troubleshooting

By collecting data, you can investigate and identify the causes of a problem, and then take the necessary measures.

This section describes details of how to collect data when a problem occurs.

9.4.1 Details of how to collecting data

The following shows how to collect data when a problem occurs.

(1) Collecting data for troubleshooting in Windows

(a) Execute the data collection tool

JP1/AJS3 for Cloud Service Applications provides the data collection tool (`jajs_log.bat`).

Use this tool if you have not changed the output destinations of log files and other data from the defaults, or if you do not need to collect data other than the data collected by default.

The following shows examples of executing the data collection tool:

```
C:\Program Files\Hitachi\JP1AJS3CSA\tools\jajs_log.bat
```

By default, the results of executing the data collection tool are output under `%TEMP%\jplajs2\backlog`. Back up these folders.

When you use the data collection tools in a cluster system, you can collect data by specifying a logical host name. The data collection tools also provide options for limiting the amount of data that is collected.

For details on the data collection tools, see *jajs_log.bat (Windows only)* in 8. *Commands*.

Important

When you execute the data collection tool, you must open the Command Prompt window as an administrator. If you are not an administrator, UAC will frequently open a confirmation dialog box.

(b) Check Windows event logs

Check Windows event logs in the **Event Viewer** pane of Windows. Also, write the logs to the file.

(c) Obtain a dump file

If a STOP error occurs in Windows or if an application crashes, you might have to obtain dump files (a memory dump and a crash dump) and a problem report.

The following describes how to obtain a dump file and a problem report.

■ How to obtain a dump file

The dump files output during the problem should be collected manually. However, in order to output a dump file when a problem occurs, it is necessary to configure the output beforehand.

Follow the procedure below to configure the dump file output.

• **Memory dump output setting procedure**

1. In Control Panel, click **System**.
The System dialog box opens.
2. Click **Advanced systems settings**.
The System Properties dialog box opens.
3. Click **Settings** button in **Startup and Recovery** on **Advanced** tab.
The Startup and Recovery dialog box opens.
4. Select the **Complete memory dump** in the **Write debugging information**, and specify the output destination file in **Dump file**.

Complete Memory Dump may not be displayed depending on the size of the installed memory. In that case, select **Kernel Memory Dump**.

Cautionary note

The memory dump size depends on the real memory size. The larger the physical memory installed, the larger the size of the memory dump. Allocate enough disk space to collect a memory dump. For details see Microsoft documentation.

• **Crash dump output setting procedure**

If a problem occurs, you may need a crash dump (a file containing debug information at the time of the problem). Windows registry information must be set in order to output a crash dump. For detailed setting information, refer to Microsoft's Windows Error Reporting (WER) related support technical information. When setting, set to output complete dump information.

Cautionary note

Crash dumps are output not only when JP1 crashes, but also when other application programs crash. In addition, when crash dumps are output, the amount of disk space is used up accordingly. Allocate sufficient disk space if you want to output crash dumps.

(d) Collect problem reports

You can detect the problem on the machine and investigate solutions for each problem. If a process on the JP1/AJS for Cloud Service Applications server stops due to an application error, follow the steps below to collect a problem report.

1. Right click Windows Start, click **Run** in Windows, enter `wercpl` in the text box, and click **OK**.
The Problem Reports and Solutions dialog box is displayed.
2. On the left pane, click **View Problem History**.
The problems history will be listed.
3. Double-click the applicable problem.
Details about the problem report appear.
4. Click **Copy to clipboard**.
5. Copy the text into a text editor, and save the file.
Use the problem report text file as data for investigating the failure.

(e) Check the status of processes

Check the operating status of the JP1/AJS3 - Manager process at the connection destination in the **Processes** tab of the Windows **Task Manager** window.

For details about the JP1/AJS3 - Manager process, see *Processes* in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

(f) Check the operation data

For the problem that has occurred, check the operation data and record it. You need to check the following information:

- Details about the operation
- Time that the problem occurred
- Machine configuration (the version of each OS, host name, JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager and JP1/AJS3 - Agent configuration)
- Whether the problem is reproducible
- Login user name for the Windows host using JP1/AJS3 for Cloud Service Applications

(g) Collect error information displayed on the screen

Make hard copies of the following:

- Windows on the screen when an application error has occurred
- Error message dialog box (and display the displayed information when a details button (if there is one) is clicked)

(h) Other information

Collect other necessary information.

- Contents of **System Information** in **Help and Support**

Print the **System Information** from **Help and Support**.

(2) Collecting data for troubleshooting in Linux

(a) Execute the data collection tool

JP1/AJS3 for Cloud Service Applications provides the data collection tool (`jaajs_log`).

Use this tool if you have not changed the output destinations of log files and other data from the defaults, or if you do not need to collect data other than the data collected by default.

The following shows examples of executing the data collection tool:

```
/opt/jp1ajs3csa/tools/jaajs_log
```

By default, the results of executing the data collection tool are output under `/tmp/jp1ajs2/trouble`.

When you use the data collection tools in a cluster system, you can collect data by specifying a logical host name. The data collection tools also provide options for limiting the amount of data that is collected.

For details on the data collection tools, see *jaajs_log (Linux only)* in *8. Commands*.

(b) Obtain the contents of the core file

Obtain the contents of the `core` file if the file has been output.

The `core` file is output to one of the following directories:

- User home directory
- Current directory in which the command was executed

(c) Check the status of server processes

Use the `ps` command to check the operating status of processes.

(d) Check the operation data

For the problem that has occurred, check the operation data and record it. You need to check the following information:

- Details about the operation
- Time that the problem occurred
- Machine configuration (the version of each OS, host name, JP1/AJS3 for Cloud Service Applications, JP1/AJS3 - Manager and JP1/AJS3 - Agent configuration)
- Whether the problem is reproducible
- Login user name for the Linux host using JP1/AJS3 for Cloud Service Applications

(e) Collect error information displayed on the screen

Make hard copies of the following:

- Windows on the screen when an application error has occurred
- Error message dialog box (and display the displayed information when a details button (if there is one) is clicked)

9.5 Troubleshooting

This section describes how to solve problems when using JP1/AJS3 for Cloud Service Applications.

9.5.1 Troubleshooting SSL communications

(1) The login screen cannot be displayed when using SSL

The following factors may be the cause.

- Your Web browser may not be configured to use SSL. Configure the Web browser to use SSL.
- Server secret key and the secret key of SSL server certificate may not match. Recreate the server secret key, Certificate Signing Request (CSR), and SSL server certificate, then restart the JP1/AJS3 CSA HTTP Server service.

(2) Errors with event source is crypt32 and event ID is 8 are output to event logs on the client machine

This error may occur when a certificate issued by a certificate authority that is not registered as a trusted root certification authority is used for SSL communication and when automatic updates by trusted root certification authority is enabled on the client machine.

This is occurring because the client machine is trying to automatically update the certificate of a trusted root certificate authority and is failing to communicate with Microsoft's Windows Update.

Take one of the following actions.

- Verify that the client machine can communicate with Windows Update provided by Microsoft.
- Disable the automatic update of the certificate by trusted root certification authority.

For information on how to disable the automatic update of the certificate by trusted root certification authority, see the Microsoft website.

9.5.2 Troubleshooting Web Browser Problems

(1) The screen is not displayed, or the display is corrupted

Make sure that you are using the operating system and Web browser that are required.

Check that the magnification of the Web browser is set to 100%.

9.5.3 Troubleshooting failures of service linkage jobs and linked cloud services

By linking a job (generation) executed on JP1/AJS3 and the linked cloud service, the following conditions can be checked.

- Check the status of the linked cloud service when a job terminates abnormally.
- Check the status of the linked cloud service while a job is running.
- Check the status of a job when the status of the linked cloud service is abnormal.

The following describes how to link a job and a cloud service:

(1) Check the status of the linked cloud service when a job terminates abnormally

Check the status of the corresponding history on the linked cloud service based on the information that the job terminated abnormally. Check the status when a job is terminated due to the time limit of job definition.

Job information to be checked

- Execution result details
- Job definition information
- Job execution information

Means to check job information

- JP1/AJS3 - View or JP1/AJS3 - Web Console
- `ajsshows` command or `ajsprint` command

(2) Check the status of the linked cloud service while a job is running

Check the status of the corresponding history on the linked cloud service based on the information of the job that is running.

Job information to be checked

- Job start date and time

Means to check job information

- JP1/AJS3 - View or JP1/AJS3 - Web Console
- `ajsshows` command

If the status cannot be identified using these means, check the status of the corresponding history on the linked cloud service based on the information output to the service linkage jobs log for a job executed by host (JP1/AJS3 - Manager host or JP1/AJS3 - Agent host) For more information about the service linkage job log, see [9.2.6 Service Linkage Job Log](#).

Service Linkage Job Log information to be checked

- CLI command run history (command line information)
- CLI start time

Means to check the service linkage job log information

- Login to job execution host (JP1/AJS3 - Manager host or JP1/AJS3 - Agent host), collect logs to check the information

(3) Check the status of a job when the status of the linked cloud service is abnormal

Check that the history corresponding to the job based on the information of the history corresponding to the linked cloud service. Check the following two items of information:

Information 1

Information on the cloud service to be checked

- Run start time
- Run finish time
- "Request IP address (job execution host)" of the corresponding request in the cloud operation logs

Means to check information on the cloud service

- Management screen of the linked cloud service

Information 2

Contents of message KNBB3034-I output to server job log

- Manager host name
- Scheduler service name
- Unit full name
- Execution ID
- Job ID

Means to check the service linkage job log information

Collect and check logs after login to JP1/AJS3 for Cloud Service Applications



Note

It is recommended that the following items be entered based on the definition of the service linkage job so that Information 1 and Information 2 can be linked, and the job can be identified from the information on the linked cloud service.

- Name of the service to be linked
- Overview of the linking process

(4) Recommended settings for service linkage job

The following settings are recommended when designing a service linkage job in order to link the job and the history of the linked cloud service.

(a) Settings of the linked cloud service

Enable the activity trace function in the linked cloud service to secure information, such as cloud operation logs.

(b) Definition of service linkage execution information

- Set the CLI command line to be output to the job's standard error output as the execution history of the CLI command. By default, the setting is to output this information.

- If the linked cloud service has an interface that enables you to specify and check arbitrary character strings, specify these strings as the information to be linked.

Specifically, the following environment variables are used.

- `AJS_CSL_JOB_UUID` (UUID set by the service linkage job)
- `AJSHOST` (Manager host name)
- `AJS_AJSCONF` (Scheduler service name)
- `AJSJOBNAME` (Job name (unit full name))
- `AJSEXECID` (Execution ID)
- `JP1JobID` (Job ID)

When specifying the manager host name, scheduler service name, job name, execution ID, and job ID, make sure that they are character strings that can be specified as CLI arguments for the linked cloud service. Pay particular attention to the value and the length of character string. For details on these environment variables, see the description of the environment variables which are configured when executing the job by JP1/AJS3 in the manual *JP1/Automatic Job Management System 3 Command Reference*.

- If there is information that can be used to identify the history on the linked cloud service side, specify that it will be output to standard error output.

Specifically, the following information should be output.

- Values that are unique to the linked cloud service (e.g., the identifier that was executed)
- URL that can refer to the status of the linked cloud service
- Information on the start time, end time, and status of the linked cloud service

9.5.4 Troubleshooting failures of service linkage monitoring jobs and linked cloud services

A service linkage monitoring job only checks the status of the linked cloud service. It does not control cloud service execution.

If the service linkage monitoring job ends abnormally after execution, or a failure occurs, such as the monitoring process continuing to run indefinitely, check for any failures that may have occurred with the cloud service.

The following settings are recommended when troubleshooting failures with the cloud service.

(1) Settings of the linked cloud service

Enable the activity trace function in the linked cloud service to secure information, such as cloud operation logs.

(2) Definition of service linkage monitoring information

- Set the CLI command line and the standard error output of the command to be output to the service linkage monitoring job log as the execution history of the CLI command executed at each monitoring interval.
They are set to be output by default.
In addition, this history is set to output to the log, regardless of whether a normal or abnormal result is returned.
- Set the CLI command line and the CLI command line standard error output to output to the detailed execution results screen if the abnormal end conditions are satisfied after executing the CLI command, and the job ends abnormally.
They are set to be output by default.

9.5.5 Troubleshooting for service linkage jobs

(1) In a Linux environment, the service linkage job was forcibly terminated unexpectedly

The size of the standard output and standard error output for the command defined for the JP1/AJS3 for Cloud Service Application server might be too large.

Check the syslog. The kernel might have stopped due to insufficient memory for the `ajscsaexec` process.

We recommend a total size of about 3 MB for the standard output and standard error output of commands defined on the JP1/AJS3 for Cloud Service Applications server. Configure the command line so that the size is not too large.

If the standard output and standard error output of commands defined on the JP1/AJS3 for Cloud Service Applications server are not required, consider specifying the command line to output to `/dev/null`.

9.5.6 Troubleshooting failures common to both service linkage jobs and service linkage monitoring jobs

(1) An unexpected value was returned as the return value for the command defined on the JP1/AJS3 for Cloud Service Applications server

The cause might be the following:

- The command does not exist in the server.
If the command is not installed, install the command.
If the command path is not set by the `PATH` environment variable, set the command path.
- The user executing the job might not have the permission to execute the command.
If the user does not have permission to execute the command, execute the job as a user who has permission.
Alternatively, change the permission required to execute the command so that the user executing the job can execute the job.
- If Windows is the OS of the execution host for the job, the command line might be too long.
Check the length of the command line and make sure that it is around 8,000 characters in length.

10

Messages

This chapter describes the messages that are issued by JP1/AJS3 for Cloud Service Applications.

10.1 JP1/AJS3 for Cloud Service Applications Messages

This section describes messages which output by JP1/AJS3 for Cloud Service Applications with message IDs.

10.1.1 Message format

Each message consists of a message ID, followed by the message text. Messages are output in one of the following formats:

Messages beginning with KNBB:

```
KNBBnnnn-Z message text
```

10.1.2 Message ID

The message ID consists of the following content:

K

System identifier

NBB

Indicates a message relating to a JP1/AJS3 for Cloud Service Applications.

nnnn

Message serial number

Z

Message type, as one of the following:

E	Error message. Processing is canceled.
I	Information message. Reports information to the user.
Q	Query message. Prompts the user to respond.
W	Warning message. Processing continues after message output.

10.1.3 Format of message explanations

Messages are explained in the following format in this manual. Characters in italic vary each time the system displays a message.

The format is as follows; however, messages with maintenance information (such as verbose error codes or file names) may be displayed without *maintenance-information* even if the message text contains *maintenance-information* in the manual.

Message ID

Message text: *message text*

Explanation of the output message text.

(S)

System action

(O)

Operator action at message output

10.2 List of output destinations for messages

This section lists the output destinations of the messages that are output by JP1/AJS3 for Cloud Service Applications.

10.2.1 Output destinations of messages beginning with KNBB

Messages whose message ID begins with KNBB are messages about JP1/AJS3 - for Cloud Service Applications. The tables in the following subsections list the output destinations for each type of message.

(1) KNBB1601 to KNBB1700 (messages about the JP1/AJS3 for Cloud Service Applications installer)

The table below lists the output destinations of messages about the JP1/AJS3 for Cloud Service Applications installer. The table uses the following abbreviations for the output destinations:

Legend:

Dialog: Message dialog box

syslog: syslog

Event log: Windows event log

App log: Application server log, application server log (for executing service linkage monitoring jobs), or application server common log

Cmd log: Command log

HNTRLib2: Integrated trace log

stdout: Standard output

stderr: Standard error output

API: API response

Web: Display on the web browser

Linkage job log: Service linkage job log

Server job log: Server job log or server job log (for executing service linkage monitoring jobs)

Y: Is output.

--: Is not output.

Table 10–1: Output destinations of messages about the JP1/AJS3 for Cloud Service Applications installer

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB1601 - KNBB1610	Y	--	--	--	--	--	--	--	--	--	--	--
KNBB1621 - KNBB1622	Y	--	--	--	--	--	--	--	--	--	--	--
KNBB1631 - KNBB1633	Y	--	--	--	--	--	--	--	--	--	--	--
KNBB1671 - KNBB1672	Y	--	--	--	--	--	--	--	--	--	--	--

(2) KNBB2001 to KNBB2500 (Web GUI messages)

Web GUI messages are displayed on a web browser.

(3) KNBB2501 to KNBB3000 (messages about JP1/AJS3 for Cloud Service Applications commands)

The table below lists the output destinations of messages about JP1/AJS3 for Cloud Service Applications commands. The table uses the following abbreviations for the output destinations:

Legend:

Dialog: Message dialog box

syslog: syslog

Event log: Windows event log

App log: Application server log, application server log (for executing service linkage monitoring jobs), or application server common log

Cmd log: Command log

HNTRLib2: Integrated trace log

stdout: Standard output

stderr: Standard error output

API: API response

Web: Display on the web browser

Linkage job log: Service linkage job log

Server job log: Server job log or server job log (for executing service linkage monitoring jobs)

Y: Is output.

--: Is not output.

Table 10–2: Output destinations of messages about JP1/AJS3 for Cloud Service Applications commands

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB2501	--	--	--	--	Y	--	--	--	--	--	--	--
KNBB2502	--	Y	Y	--	Y	Y	Y	--	--	--	--	--
KNBB2503	--	Y	Y	--	Y	Y	--	Y	--	--	--	--
KNBB2504 - KNBB2505	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2506	--	--	--	--	Y	--	--	--	--	--	--	--
KNBB2507	--	Y	Y	--	Y	Y	Y	--	--	--	--	--
KNBB2511 - KNBB2516	--	--	--	--	Y	--	--	--	--	--	--	--
KNBB2517 - KNBB2519	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2520 - KNBB2521	--	--	--	--	Y	--	Y	--	--	--	--	--

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB2522 - KNBB2525	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2526	--	--	--	--	Y	--	--	--	--	--	--	--
KNBB2528 - KNBB2529	--	--	--	--	Y	--	--	--	--	--	--	--
KNBB2551 - KNBB2552	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2554	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2556	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2558	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2601	--	Y	Y	--	Y	--	--	Y	--	--	--	--
KNBB2602 - KNBB2603	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2651 - KNBB2655	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2657 - KNBB2660	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2701	--	--	--	--	--	--	Y	--	--	--	--	--
KNBB2702	--	--	--	--	Y	--	Y	--	--	--	--	--
KNBB2703	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2708	--	--	--	--	Y	Y	--	Y	--	--	--	--
KNBB2709 - KNBB2710	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2712	--	--	--	--	Y	--	--	Y	--	--	--	--
KNBB2714 - KNBB2715	--	--	--	--	Y	--	--	Y	--	--	--	--

(4) KNBB3001 to KNBB3999 (messages about the web application server)

The table below lists the output destinations of messages about the web application server. The table uses the following abbreviations for the output destinations:

Legend:

Dialog: Message dialog box

syslog: syslog

Event log: Windows event log

App log: Application server log, application server log (for executing service linkage monitoring jobs), or application server common log

Cmd log: Command log

HNTRLib2: Integrated trace log

stdout: Standard output

stderr: Standard error output

API: API response

Web: Display on the web browser

Linkage job log: Service linkage job log

Server job log: Server job log or server job log (for executing service linkage monitoring jobs)

Y: Is output.

--: Is not output.

Table 10–3: Output destinations of messages about the web application server

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB3001 - KNBB3006	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3026 - KNBB3031	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3033	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3034	--	--	--	--	--	--	--	--	--	--	--	Y
KNBB3035	--	--	--	--	--	--	--	--	--	--	--	Y
KNBB3051 - KNBB3052	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3054 - KNBB3056	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3059 - KNBB3064	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3102	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3103 - KNBB3106	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3151 - KNBB3153	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3208	--	--	--	Y	--	--	--	--	Y	--	--	--
KNBB3212	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3216	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3238 - KNBB3240	--	--	--	Y	--	--	--	--	Y	--	--	--
KNBB3290	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3291	--	--	--	Y	--	--	--	--	Y	--	--	--
KNBB3609	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3669	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3689	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB3801 - KNBB3806	--	--	--	Y	--	--	--	--	--	--	--	--

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB3807 - KNBB3808	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3901 - KNBB3903	--	--	--	Y	--	--	--	--	Y	Y	--	--
KNBB3905	--	--	--	Y	--	--	--	--	--	--	--	--

(5) KNBB4000 to KNBB4500 (messages about the Service linkage job definition screen or the Service linkage monitoring job definition screen)

Messages about the Service linkage job definition screen or the Service linkage monitoring job definition screen are displayed on the dialog box of JP1/AJS3 - View.

(6) KNBB4501 to KNBB5000 (messages about the service linkage job or service linkage monitoring job definitions commands)

The table below lists the output destinations of messages about the service linkage job or service linkage monitoring job definitions commands. The table uses the following abbreviations for the output destinations:

Legend:

Dialog: Message dialog box

syslog: syslog

Event log: Windows event log

App log: Application server log, application server log (for executing service linkage monitoring jobs), or application server common log

Cmd log: Command log

HNTRLib2: Integrated trace log

stdout: Standard output

stderr: Standard error output

API: API response

Web: Display on the web browser

Linkage job log: Service linkage job log

Server job log: Server job log or server job log (for executing service linkage monitoring jobs)

Y: Is output.

--: Is not output.

Table 10–4: Output destinations of messages about the service linkage job or service linkage monitoring job definitions commands

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB4501	--	--	--	--	--	--	Y	--	--	--	--	--

Message ID	Output destination											
	Dialog	syslog	Event log	App log	Cmd log	HNTRLib2	stdout	stderr	API	Web	Linkage job log	Server job log
KNBB4502 - KNBB4509	--	--	--	--	--	--	--	Y	--	--	--	--
KNBB4511 - KNBB4514	--	--	--	--	--	--	--	Y	--	--	--	--
KNBB4515	--	--	--	--	--	--	Y	--	--	--	--	--
KNBB4516 - KNBB4526	--	--	--	--	--	--	--	Y	--	--	--	--

(7) KNBB6000 to KNBB6499 (messages about the service linkage job execution programs or the service linkage monitoring job execution programs)

The table below lists the output destinations of messages about the service linkage job execution programs or the service linkage monitoring job execution programs.

The table uses the following abbreviations for the output destinations:

Legend:

Dialog: Message dialog box

syslog: syslog

Event log: Windows event log

App log: Application server log, application server log (for executing service linkage monitoring jobs) or application server common log

Cmd log: Command log

HNTRLib2: Integrated trace log

stdout: Standard output

stderr: Standard error output

API: API response

Web: Display on the web browser

Linkage job log: Service linkage job log

Server job log: Server job log or server job log (for executing service linkage monitoring jobs)

Execution result details: Execution result details dialog box in JP1/AJS3 - View or JP1/AJS3 - Web Console

Objects monitoring job log: Service linkage objects monitoring job log

Y: Is output.

--: Is not output.

Table 10–5: Output destinations of messages about the service linkage job execution programs or the service linkage monitoring job execution programs

Message ID	Output destination													
	Dialo g	syslo g	Eve nt log	Ap p lo g	Cm d log	HNTRLi b2	stdo ut	stde rr	A PI	We b	Linka ge job log	Serv er job log	Executi on result details	Objects monitori ng job log
KNBB6000 - KNBB6001	--	--	--	--	--	--	--	--	--	--	Y	--	--	--
KNBB6002 - KNBB6003	--	--	--	--	--	--	--	--	--	--	Y	--	--	Y
KNBB6004	--	--	--	--	--	--	--	Y#1	--	--	Y#1	--	Y#1	Y
KNBB6005	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6011 - KNBB6012	--	--	--	--	--	Y	--	--	--	--	--	--	--	Y
KNBB6013 - KNBB6018	--	--	--	--	--	--	--	--	--	--	--	--	Y	--
KNBB6100	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	Y
KNBB6101	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	--
KNBB6102	--	--	--	--	--	--	--	--	--	--	--	--	--	Y
KNBB6103	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6104	--	--	--	--	--	--	--	--	--	--	--	--	Y	--
KNBB6105 - KNBB6107	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6150 - KNBB6154	--	--	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB6155 - KNBB6156	--	--	--	--	--	Y	--	--	--	--	--	--	Y	--

Message ID	Output destination													
	Dialog	syslog	Event log	App log	Cmd log	HNTRLi b2	stdout	stderr	API	Web	Linkage job log	Server job log	Execution result details	Objects monitoring job log
KNBB6157 - KNBB6162	--	--	--	--	--	Y	--	--	--	--	--	--	--	--
KNBB6163 - KNBB6164	--	--	--	--	--	Y	--	--	--	--	--	--	Y	--
KNBB6200 - KNBB6204	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	Y
KNBB6205	--	--	--	--	--	--	--	--	--	--	Y	--	Y	--
KNBB6300	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	Y
KNBB6301 - KNBB6305	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	--
KNBB6306	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6307	--	--	--	--	--	--	--	--	--	--	--	--	--	Y
KNBB6308	--	--	--	--	--	Y	--	--	--	--	--	--	--	Y
KNBB6309 - KNBB6312	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6400 - KNBB6401	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	--
KNBB6402 - KNBB6403	--	--	--	--	--	Y	--	--	--	--	--	--	--	Y
KNBB6449	--	--	--	--	--	--	--	--	--	--	--	--	Y	Y
KNBB6450	--	--	--	--	--	--	--	Y	--	--	Y	--	Y	Y
KNBB6451 - KNBB6452	--	--	--	--	--	Y#2	--	Y	--	--	Y	--	Y	Y

Note:

Messages with a message ID of KNBB6000 to KNBB6499 are not output for service linkage monitoring jobs.

#1:

Output only if you check **Output the executed command line** in **Trace information settings** in JP1/AJS3 for Cloud Service Applications.

#2:

Even for messages output to the integrated trace log, messages output from service linkage objects monitoring jobs may only be output to detailed execution results or service linkage objects monitoring job logs, without being output to the integrated trace log.

10.3 List of messages

This section lists messages which output by JP1/AJS3 for Cloud Service Applications with message IDs.

10.3.1 Messages beginning with KNBB

This section explains the messages that begin with KNBB (messages about JP1/AJS3 for Cloud Service Applications).

(1) List of messages that begin with KNBB (messages about the JP1/AJS3 for Cloud Service Applications installer)

The following is a list of messages that begin with KNBB (messages about the JP1/AJS3 for Cloud Service Applications installer):

KNBB1601-E

This platform is not supported. Installation stops.

The installation was interrupted because an attempt was made to install a JP1/AJS3 product on a platform that does not meet the applicable operating system requirements. The JP1/AJS3 product cannot be installed on this platform.

(S)

The system aborts the installation.

(O)

Check the applicable operating system for the JP1/AJS3 product and install it on that OS.

For information on the applicable operating system, see the *release notes*.

KNBB1603-E

The Hitachi Integrated Installer disc might be corrupted. Installation cannot continue.

Installation was interrupted because an error occurred during installation.

The following factors may have caused the problem.

- Disc defect of Hitachi Integrated Installer
- If you are using the Hitachi Integrated Installer copied to a local disc, copying has failed.

(S)

The system aborts the installation.

(O)

If you have another Hitachi Integrated Installer disc, install JP1/AJS3 again using this disc.

If you are using the Hitachi Integrated Installer copied to a local disc, copy it again and install JP1/AJS3. Or, install JP1/AJS3 using the Hitachi Integrated Installer disc.

If the problem persists, collect the following data and contact your system administrator.

- Details of the operation performed
- Dialog displayed on the screen

- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1604-E

Setting of license management information failed. The installation will stop.*(maintenance-information)*

The installation was interrupted because the license management information failed to be set.

(S)

The system aborts the installation.

(O)

Collect the following data and contact your system administrator.

- Details of the operation performed
- Dialog displayed on the screen
- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1606-E

The user who executed the installation is not an administrator. An administrator is required to install this product.

The installation could not be performed because the user who performed the installation does not have administrative privileges.

(S)

The system aborts the installation.

(O)

A user who has administrative privileges should install JP1/AJS3 products.

KNBB1607-E

An internal error occurred during AJS3 setup. *(maintenance-information)*

An error occurred during the setup that JP1/AJS3 automatically performs during installation.

The following factors may be the cause:

- The port number used by JP1/AJS3 for Cloud Service Applications is already being used by another program.
- Insufficient capacity on the system drive (%systemdrive%).
- Insufficient capacity on the destination drive for the installation.

(S)

The system aborts the installation.

(O)

Eliminate the cause and reinstall JP1/AJS3.

If the problem persists, collect the following data and contact your system administrator.

- Details of the operation performed
- Hard copy of the dialog box displayed on the screen
- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1608-E

Error occurred at opening file .Installation stops. (*maintenance-information*)

The installation was interrupted because the file used in the installation could not be opened.

The following factors may be the cause:

- Insufficient capacity on the system drive (%systemdrive%)
- The folder set in the system environment variable TEMP does not have write or read permissions.

Note: The file name that caused the error is output to maintenance information.

(S)

The system aborts the installation.

(O)

Eliminate the cause and reinstall JP1/AJS3.

If the problem persists, collect the following data and contact your system administrator.

- Details of the operation performed
- Dialog displayed on the screen
- Click **Properties** and **Security** of the folder set in the system environment variable TEMP, and make a hard copy of the Security screen.
- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1609-E

Error occurred at reading file. Installation stops. (*maintenance-information*)

The installation was interrupted because the file used in the installation could not be read.

The following factors may be the cause:

- The folder set in the system environment variable TEMP does not have read permissions.

Note: The file name that caused the error is output to maintenance information.

(S)

The system aborts the installation.

(O)

Eliminate the cause and reinstall JP1/AJS3.

If the problem persists, collect the following data and contact your system administrator.

- Details of the operation performed
- Dialog displayed on the screen
- Click **Properties** and **Security** of the folder set in the system environment variable TEMP, and make a hard copy of the Security screen.
- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1610-E

An internal error occurred during AJS3 unsetup. (*maintenance-information*)

An error occurred during the unsetup process automatically performed by JP1/AJS3 during uninstallation.

The following factors may be the cause:

- An invalid value is set in the preferences file.
- Files required for uninstallation have been deleted.

(S)

The system aborts the installation.

(O)

If an invalid value is set in the preferences file, enter the correct value. Otherwise, overwrite the installation once and uninstall again.

If the problem persists, collect the following data and contact your system administrator.

- Details of the operation performed
- Make a hard copy of the dialog box displayed on the screen
- Execution results of the data collection tool

KNBB1621-E

JP1/Base is not installed. Install JP1/Base, and then install AJS3.

Installation failed because JP1/Base is not installed.

(S)

The system aborts the installation.

(O)

Install JP1/Base version meets the prerequisites, and then restart the installation of AJS3. For the required JP1/Base version, see the *release notes*.

KNBB1622-E

The version of the installed JP1/Base is old. Please install after installing *JP1/Base-version-information* or later.

The installation was interrupted because the version of JP1/Base installed does not meet the prerequisite requirements of the product.

(S)

The system aborts the installation.

(O)

Install JP1/Base version meets the prerequisites, and then restart the installation of AJS3. For the required JP1/Base version, see the *release notes*.

KNBB1671-Q

The Hitachi Integrated Installer disc could not be found. Insert the disc into the drive.

The system checks for files on the Hitachi Integrated Installer disc that cannot be found.

(S)

The system waits for the response.

(O)

If you wish to continue the installation, select **Yes** after inserting the Hitachi Integrated Installer disc into the drive.

If you do not wish to continue the installation, select **No** to terminate the installation.

If the problem persists after inserting the Hitachi Integrated Installer disc, collect the following data and contact your system administrator.

- Details of the operation performed
- Dialog displayed on the screen
- Installation log

If overwriting the installation or upgrading the installation, collect the following data as well.

- Execution results of the data collection tool

KNBB1672-Q

This platform is not an applicable OS. Do you want to stop the installation?

The system confirms that the product installation is on a platform that meets the applicable OS requirements.

(S)

The system waits for the response.

(O)

Click the **Yes** button to finish the installation.

(2) List of messages that begin with KNBB (Web GUI messages)

The following is a list of messages that begin with KNBB (Web GUI messages):

KNBB2001-E

Specify *field-name*.

field-name is not specified.

(S)

The system aborts the process.

(O)

Enter the value in *field-name* and try again.

KNBB2003-E

Enter the values *minimum-value - maximum-value* in *field-name*.

The value was entered incorrectly in *field-name*.

(S)

The system aborts the process.

(O)

Re-enter the value of *minimum-value - maximum-value* in *field-name*.

KNBB2004-E

The *field-name* is specified incorrectly.

Incorrect format value is specified in *field-name*.

(S)

The system aborts the process.

(O)

Re-enter the correct format value in *field-name*.

KNBB2005-E

Duplicate variable name (*variable-name*).

The registration of the definition failed because the variable name is duplicated.

(S)

The system aborts the process.

(O)

Remove the duplicate variable name and click the **Register** button.

KNBB2006-E

Invalid import file format.

The import failed because the format of the definition file to be imported is invalid. If a value that cannot be entered is specified for the JSON key that corresponds to the input or specified value on each screen, the text field shows the values that can be read[#] and the checkbox or radio button shows the default value.

[#]: If the file contains characters that cannot be read properly by the Web browser, the characters will be garbled and displayed on the screen.

(S)

The system aborts the process.

- (O)
- Check that the file specified below is the exported file from the relevant definition screen and import it.
- The file must be in JSON format.
 - The file must be the one exported from the relevant definition screen.

KNBB2007-E

The maximum number (*maximum-value*) of variables that can be set for *item-name* was exceeded.

The registration of the definition failed because the variable exceeded the maximum value.

- (S)
- The system aborts the process.

- (O)
- Delete the variable and click the **Register** button.
- The maximum values of variables that can be registered are as follows:
- Custom input items for JP1/AJS3 - View
15 items
 - Environment variables for the execution host
32 items

KNBB2008-E

The user name or password is invalid.

Login failed because the value entered for the JP1 username or password was invalid.

- (S)
- The system aborts the process.

- (O)
- Make sure that the value entered is valid, and enter the JP1 username and password registered on the Access Control Server to which it is connected, and then log in.

KNBB2101-E

Cannot connect to the Server.

This message reports that access to the JP1/AJS3 for Cloud Service Applications server application failed. The following factors may be the cause.

- An error occurred during the communication process with the HTTP server or application server.
- The HTTP server or application server is not running.
- The HTTP server or application server is busy.
- The HTTP server or application server is not ready to connect the network.

- (S)
- The system aborts the process.

(O)

- An error occurred during the communication process with the HTTP server or application server.
Eliminate the cause of the errors and log in to JP1/AJS3 for Cloud Service Applications.
- The HTTP server or application server is not running.
Check either the JP1/AJS3 CSA HTTP Server service or JP1/AJS3 CSA Web Application Server service is running. If it is stopped, restart it and log in again.
- The HTTP server or the application server is busy.
It may be connected by retrying the connection.
- The network connection to the HTTP server or application server is not available.
Check the network environment with the HTTP server or application server. If there is a firewall between the HTTP server or the application server, check the firewall settings. If the session has been terminated, log in again.

KNBB2401-Q

Are you sure you want to log out?

The system confirms that you want to log out from JP1/AJS3 for Cloud Service Applications.

(S)

The system waits for the response.

(O)

Click the **OK** button to log out or click the **Cancel** button to cancel.

KNBB2402-Q

Are you sure you want to delete the *definition-type "definition-name"*?

The system confirms that you will delete the definition *definition-name*.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition
- object monitoring definition

(S)

Waits for a response.

(O)

Click the **OK** button to delete or click the **Cancel** button to cancel.

KNBB2407-Q

This is a definition (*definition-type "definition-name"*) that has a job execution history. Do you want to update it?

The system confirms whether to continue updating the definition if a service linkage job or service linkage monitoring job using the definition to be updated has been executed by JP1/AJS3 - Manager.

A *definition-type* displays one of the following:

- service linkage job definition
- authentication definition
- service linkage monitoring job definition

(S)

Waits for a response.

(O)

Click the **OK** button to update or click the **Cancel** button to cancel.

To identify JP1/AJS3 - Manager jobs, use the following method:

- Identify the job that uses the target definition from KNBB3034-I in the server jobs log of JP1/AJS3 for Cloud Service Applications.
- From the unit definition of JP1/AJS3 - Manager that defines the service linkage job, identify the job by checking either of the following parameters that indicate the service linkage job definition name or the authentication definition name.
 - env="AJS_CSA_DEFINFNAME=*service-linkage-job-definition-name*";
 - env="AJS_CSA_AUTHINFNAME=*authentication-definition-name*";
- From the unit definition of JP1/AJS3 - Manager that defines the service linkage monitoring job, identify the job by checking either of the following parameters that indicate the service linkage monitoring job definition name or the authentication definition name.
 - cprm="AJS_CSA_MONDEFINFNAME=*service-linkage-monitoring-job-name*";
 - cprm="AJS_CSA_AUTHINFNAME=*authentication-definition-name*";

KNBB2408-Q

This is a definition (*definition-type "definition-name"*) that has a job execution history. Do you want to delete it?

A service linkage job or service linkage monitoring job using the definition to be deleted has been executed in JP1/AJS3 - Manager.

The system confirms whether you really want to delete the file or not, since deleting it may affect JP1/AJS3 - Manager jobs.

A *definition-type* displays one of the following:

- service linkage job definition
- authentication definition
- service linkage monitoring job definition

(S)

Waits for a response.

(O)

Click the **OK** button to delete or click the **Cancel** button to cancel.

To identify JP1/AJS3 - Manager jobs, use the following method:

- Identify the job that uses the target definition from KNBB3034-I in the server jobs log of JP1/AJS3 for Cloud Service Applications.
- From the unit definition of JP1/AJS3 - Manager that defines the service linkage job, identify the job by checking either of the following parameters that indicate the service linkage job definition name or the authentication definition name.
 - env="AJS_CSA_DEFINFNAME=*service-linkage-job-definition-name*";
 - env="AJS_CSA_AUTHINFNAME=*authentication-definition-name*";
- From the unit definition of JP1/AJS3 - Manager that defines the service linkage monitoring job, identify the job by checking either of the following parameters that indicate the service linkage monitoring job definition name or the authentication definition name.
 - cprm="AJS_CSA_MONDEFINAME=*service-linkage-monitoring-job-definition-name*";
 - cprm="AJS_CSA_AUTHINFNAME=*authentication-definition-name*";

KNBB2409-Q

This is the definition (*definition-type "definition-name"*) used in the *job-definition-type*. Do you want to update it?

Applications. The system confirms whether you really want to update the definition or not, since deleting it may affect the running job.

This definition is used in JP1/AJS3 for Cloud Service Applications job definitions. The system confirms whether you really want to update the definition or not, since this may affect the job running.

A *job-definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- service linkage job definition or service linkage monitoring job definition

A *definition-type* displays one of the following:

- connection definition
- object monitoring definition

(S)

Waits for a response.

(O)

Click the **OK** button to update or click the **Cancel** button to cancel.

To confirm the operation using the definition, check the contents from the definition screen of the job definitions.

KNBB2410-Q

This is the definition (*definition-type "definition-name"*) used in the *job-definition-type*. Do you want to delete it?

This definition is used for the job definitions for JP1/AJS3 for Cloud Service Applications. The system confirms whether you really want to delete the definition or not, since deleting it may affect the job running.

A *job-definition-type* displays one of the following:

- service linkage job definition

- service linkage monitoring job definition
- service linkage job definition or service linkage monitoring job definition

A *definition-type* displays one of the following:

- connection definition
- execution definition
- object monitoring definition

(S)

Waits for a response.

(O)

Click the **OK** button to delete or click the **Cancel** button to cancel.

To confirm the operation using the definition, check the contents from the definition screen of the job definitions.

KNBB2411-E

definition-type "definition-name" already exists.

The registration of the definition failed because the definition type has already been registered.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition
- object monitoring definition

(S)

The system aborts the process.

(O)

Change the definition name and click the **Register** button again.

KNBB2412-I

definition-type "definition-name" was registered.

The definition was registered successfully.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition

- object monitoring definition

(S)

Waits for a response.

KNBB2413-I

definition-type "definition-name" was deleted.

The definition was deleted successfully.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition
- object monitoring definition

(S)

Waits for a response.

KNBB2414-E

The session you logged in to is disabled. Export the definition being created and then log in again as needed.

The logged-in session is already invalid. If necessary, export the definitions to temporarily save the definitions being created, then log in again.

The exported definitions can be imported to the screen by the import function of the corresponding definition screen.

(S)

The system aborts the process.

(O)

If necessary, export the definitions temporarily to save it being created, then log in again and retry the operation.

KNBB2415-E

No authority for *definition-type "definition-name"*.

The operation failed because there is insufficient permission for the operation-target definition of the definition type.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition

- object monitoring definition

(S)

The system aborts the process.

(O)

Check the JP1 resource group settings of the operation-target definition, add the permissions, and then perform the operation.

KNBB2416-W

Registration was not performed by using the registered value because the definition was deleted. Check the value of the item for which "Protect" is specified. (Item name: *item-name*)

After opening a registered authentication definition from the Home screen, it was deleted before registration. Since the previous value that had been registered has been deleted, input items that do not select **Update Value** will be registered as if they had not been entered.

Enter the original values, check the **Update Value** checkbox, and then confirm that the registration is ready.

(S)

The system continues.

(O)

Please confirm the value that was entered in the item that has been checked in **Protect** and register again.

KNBB2417-E

definition-type "definition-name" has already been deleted.

Deletion and loading of the definition failed because the definition of the registered definition type has already been deleted.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition
- object monitoring definition

(S)

The system aborts the process.

(O)

Refresh the screen to display the latest definition list screen and then perform the operation.

(3) List of messages beginning with KNBB (messages about JP1/AJS3 for Cloud Service Applications commands)

The following is a list of messages beginning with KNBB (messages about JP1/AJS3 for Cloud Service Applications commands):

KNBB2418-W

The definition "*definition-name*", which cannot be specified for the *definition-type*, is selected.

The definition could not be specified because either the connection definition or the execution definition specified in the service linkage job definition was deleted, or the user does not have reference permissions.

The definition could not be specified because either the connection definition or the monitoring definition specified in the service linkage monitoring job definition was deleted, or the user does not have reference permissions.

A *definition-type* displays one of the following:

- connection definition
- execution definition
- object monitoring definition

(S)

The system aborts the process.

(O)

Register the definition, and then either reopen the definition, or import it to load the definition.

KNBB2419-W

You will be redirected to the home screen because of an invalid operation.

You will be redirected to the home screen because the browser's **Back** or **Forward** button was used.

(S)

The system aborts the process.

(O)

Retry the operation from the home screen.

KNBB2501-I

The service (*service*) will now start.

Start Service (*service*).

(S)

Continues processing.

KNBB2502-I

The service (*service*) started.

Service started successfully.

(S)

The system outputs the fact that the service has started to the log.

KNBB2503-E

The service (*service*) failed to start.

The start failed because an error occurred during the service startup process.

(S)

The system aborts the service startup process.

(O)

Before this message is displayed, the message indicating the error is output to the command log or the application server log. Take action according to the message that was output immediately before this message.

KNBB2504-W

The service (*service*) is already running.

This message is output when the service attempting to start has already been started. Skip the startup process of the service that has already started and continue the process.

(S)

Continues processing.

KNBB2505-W

The service (*service*) is not running.

This message is output when the service attempting to stop has already been stopped. Skip the stop process of the service that has already stopped and continue the process.

(S)

Continues processing.

KNBB2506-I

The service (*service*) will now stop.

The system stops the service.

(S)

Continues processing.

KNBB2507-I

The service (*service*) has terminated.

Service is terminated.

(S)

The system outputs to the log that the service has been terminated.

KNBB2511-I

Setup of CSA started.

The system started the setup of JP1/AJS3 for Cloud Service Applications.

(S)

Continues processing.

KNBB2512-I

Setup of CSA ended successfully.

The system successfully completed the setup of JP1/AJS3 for Cloud Service Applications.

(S)

Continues processing.

KNBB2513-E

Failed to set up CSA

The system failed to setup JP1/AJS3 for Cloud Service Applications.

(S)

The system aborts command execution.

(O)

Before this message is displayed, the message indicating the error is output to the command log. Take action according to the message that was output immediately before this message.

KNBB2514-I

Unsetup of CSA started.

The system started the unsetup of JP1/AJS3 for Cloud Service Applications.

(S)

Continues processing.

KNBB2515-I

Unsetup of CSA ended successfully.

The system failed the unsetup of JP1/AJS3 for Cloud Service Applications.

(S)

Continues processing.

KNBB2516-E

Failed to perform unsetup of CSA.

The system failed the unsetup of JP1/AJS3 for Cloud Service Applications.

(S)

The system aborts command execution.

(O)

Before this message is displayed, the message indicating the error is output to the command log. Take action according to the message that was output immediately before this message.

KNBB2517-E

A system error has occurred. : *maintenance-information*

A system error occurred during processing. There may be a problem with the execution environment of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process in which the error occurred.

(O)

Use the data collection tool to collect data, and then contact the system administrator.

KNBB2518-E

Insufficient memory occurred. : *maintenance-information-1 maintenance-information-2 maintenance-information-3 maintenance-information-4*

Insufficient memory was detected in the execution environment of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process in which the error occurred.

(O)

Check the physical memory usage of the host where the JP1/AJS3 CSA Web Application Server service is running. If the capacity of the available physical memory is insufficient, terminate unnecessary applications to increase the size of available physical memory. (For details of the required capacity of physical memory of JP1/AJS3 for Cloud Service Applications, see the *release notes*.)

KNBB2519-E

Unexpected error occurred in CSA. : *maintenance-information-1 maintenance-information-2 maintenance-information-3 maintenance-information-4*

An unexpected error occurred during processing. There may be a problem with the execution environment of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process in which the error occurred.

(O)

Use the data collection tool to collect data, and then contact the system administrator.

KNBB2520-I

Output of settings data will now start.

The system starts outputting settings data.

(S)

Continues processing.

KNBB2521-I

Output of settings data ended.

The system finished outputting settings data.

(S)

Continues processing.

KNBB2522-E

A timeout occurred while the service(*service*) was being started. (maintenance information = *maintenance-information-1*)

The startup process of the service failed because a timeout occurred during the startup process.

(S)

The system aborts the service startup process.

(O)

Eliminate the cause of the timeout, such as system startup or a temporarily high load, and execute the process again.

KNBB2523-E

A timeout occurred while the service(*service*) was being stopped. (maintenance information = *maintenance-information-1, maintenance-information-2*)

The stop process of the service failed because a timeout occurred during its stop process.

(S)

The system aborts the service stop processing.

(O)

Eliminate the cause of the timeout, such as system startup or a temporarily high load, and execute the process again.

KNBB2524-E

An error occurred while the service (*service*) was being started. (maintenance information = *maintenance-information-1, maintenance-information-2*)

The startup process of the service failed because an error occurred during the startup process. The following may be the cause.

- There is an error in the definition file.
- Timeout occurred.
- JP1/AJS3 CSA HTTP Server was started twice (when the service is operated by JP1/AJS3 CSA HTTP Server).

(S)

The system aborts the service startup process.

(O)

Eliminate the cause of the error and execute the process again.

KNBB2525-E

An error occurred while the service (*service*) was being stopped. (maintenance information = *maintenance-information-1, maintenance-information-2, maintenance-information-3, maintenance-information-4*)

The stop process of the service failed because an error occurred during its stop process. The following may be the cause.

- There is an error in the definition file.
- Timeout occurred.

(S)

The system aborts the service stop processing.

(O)

Eliminate the cause of the error and execute the process again.

KNBB2526-I

SERVICE : *maintenance-information*

This message is to report the progress of the service startup and stop processes.

(S)

The system outputs the progress of service startup and stop processes to the log.

KNBB2528-W

Setup of the CSA ended with warning.

This message is output when the initialization of the log, which is output by the setup process, has failed.

(S)

Continues processing.

(O)

The log may not be output during the setup process, but no action is required because the setup is complete.

KNBB2529-W

Unsetup of the CSA ended with warning.

This message is output when the initialization of the log, which is output by the unsetup process, has failed.

(S)

Continues processing.

(O)

The log may not be output during the unsetup process, but no action is required because the unsetup is complete.

KNBB2551-E

Failed to load the environment configuration file.

The process was aborted because loading of the environment configuration file failed.

(S)

The system aborts the process in which the error occurred.

(O)

Make sure that the environment configuration file has the privilege to be loaded. If not, change the setting and execute again.

If the failure occurred when starting the service, stop the JP1/AJS3 CSA HTTP Server service, restart the JP1/AJS3 CSA Web Application Server service, and then start the JP1/AJS3 CSA HTTP Server service.

KNBB2552-E

The environment configuration file contains incorrect specifications. (*detailed-information*)

The process was aborted because an incorrect specification was made in the environment configuration file.

(S)

The system aborts the process in which the error occurred.

(O)

Set the environment configuration file correctly. If not, change the setting and execute again.

Make sure that the environment configuration file has the privilege to be loaded. If not, change the setting and execute again.

If the failure occurred when starting the service, stop the JP1/AJS3 CSA HTTP Server service, restart the JP1/AJS3 CSA Web Application Server service, and then start the JP1/AJS3 CSA HTTP Server service.

KNBB2554-E

The shared directory is specified incorrectly. (*shared-directory*)

There is an incorrect setting in the logical host. The following may be the cause.

- The configured shared directory does not exist.
- The length of the name of the configured shared directory exceeds the maximum value.

(S)

The system aborts the process in which the error occurred.

(O)

Confirm that the configured shared directory is available.

KNBB2556-E

The same command cannot be executed redundantly.

The process was interrupted because commands were executed concurrently.

(S)

The system aborts the process in which the error occurred.

(O)

An error may occur when commands are executed at the same time. If an error occurs, execute the process again.

KNBB2558-E

I/O error occurred. (*file-name*) : *maintenance-information-1 maintenance-information-2 maintenance-information-3 maintenance-information-4*

An error occurred during file input or output. The following may be the cause.

- The user does not have access privileges to the file.
- The file is being used by another process.

(S)

The system aborts the process in which the error occurred.

(O)

Eliminate the cause of the error and execute the process again.

KNBB2601-E

The log output processing could not be initialized. Detailed information (*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4*)

The initialization of the integrated trace log and command log failed.

(S)

The system aborts the startup process for the JP1/AJS3 CSA Web Application Server service on Windows. Otherwise, the system continues the process.

(O)

If an error message related to the environment configuration file has been output before this message is displayed, take action according to the error message. Otherwise, collect the data by using the data collection tool and contact your system administrator.

KNBB2602-W

The log could not be output. Detailed information (*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4*)

Output of the integrated trace log failed. There may be a problem with the integrated trace function.

(S)

The system aborts the output of the integrated trace log and continues the process.

(O)

Use the data collection tool to collect data, and then contact the system administrator.

KNBB2603-W

Log output processing failed to complete. Detailed information (*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4*)

Completion of the integrated trace log output process failed.

(S)

Continues processing.

(O)

Use the data collection tool to collect data, and then contact the system administrator.

KNBB2651-E

Illegal option (*option*) exists.

An inappropriate option is specified.

(S)

The system aborts command execution.

(O)

Specify the correct option and rerun the command.

KNBB2652-E

Value for option (*option*) is not specified.

A value was not specified for an option that requires a value.

(S)

The system aborts command execution.

(O)

Specify the value of the option and rerun the command.

KNBB2653-E

Invalid value for option (*option*).

The value of the option was specified incorrectly.

(S)

The system aborts command execution.

(O)

Specify the value of the option and rerun the command.

KNBB2654-E

Option (*option*) appears twice or more.

The same option is specified twice or more.

(S)

The system aborts command execution.

(O)

Correct the option specified twice or more to only once and rerun the command.

KNBB2655-E

The specified argument is incorrect.

The incorrect argument is specified.

(S)

The system aborts command execution.

(O)

Correct the argument and rerun the command.

KNBB2657-E

Failed to access shared directory.

Access to the shared directory failed.

(S)

The system aborts command execution.

(O)

Check whether the specified shared directory exists. If it exists, check whether there are the reference privilege and the update privilege in the specified shared directory.

KNBB2658-E

Failed to create shared directory (*directory-name*).

The creation of the shared directory failed.

(S)

The system aborts command execution.

(O)

Check that the `jp1ajs3csa` directory, which is displayed in the message, does not exist.

Windows:

`specified-shared-directory-name\jp1ajs3csa`

UNIX:

`specified-shared-directory-name/jp1ajs3csa`

If the `jp1ajs3csa` directory exists, confirm that the specified shared directory name is correct. If it is correct, confirm that the `jp1ajs3csa` directory is unnecessary, and delete it, then rerun the command (do not delete the shared directory).

If there is no `jp1ajs3csa` directory, confirm that the specified shared directory has update privileges.

KNBB2659-E

Logic host (*logical-host*) is not found.

The process was aborted because the logical host could not be found.

(S)

The system aborts command execution.

(O)

Check whether the specified logical host is defined in JP1/Base.

KNBB2660-E

Only super user or administrator can execute.

A user without superuser or administrator privileges tried to run the command.

(S)

The system aborts command execution.

(O)

A user with superuser or administrator privileges must run the command.

If the UAC function is enabled on Windows, a user with administrator privilege should rerun the command.

KNBB2701-I

The command (*command*) started.

Start processing the command (*command*).

(S)

Continues processing.

KNBB2702-I

The command (*command*) ended normally.

The processing of the command (*command*) has ended normally.

(S)

The system outputs to the log that the command has ended normally.

KNBB2703-E

The command (*command*) ended abnormally.

The processing of the command (*command*) has ended abnormally.

(S)

The system outputs to the log that the command has ended abnormally.

(O)

Before this message is displayed, the message indicating the error is output to the standard error output. Investigate the cause based on those messages.

KNBB2708-E

The expiration of the time limit. CSA

The evaluation version has exceeded its expiration date.

(S)

The system aborts the process of starting the JP1/AJS3 CSA Web Application Server service.

KNBB2709-E

CSA service is set up already.

The setup process of JP1/AJS3 for Cloud Service Applications was not performed because its service has already been set up.

(S)

The system terminates the setup process.

(O)

Make sure that the JP1/AJS3 for Cloud Service Applications service has been set up.

KNBB2710-E

An error occurred during installing CSA service. : *maintenance-information-1 maintenance-information-2 maintenance-information-3 maintenance-information-4*

An error occurred during the setup of the JP1/AJS3 for Cloud Service Applications service. There may be a problem with the execution environment of the JP1/AJS3 for Cloud Service Applications service.

(S)

The system terminates the setup process.

(O)

Run the setup command as an OS user with Administrator privileges. If the UAC function is enabled on Windows, a user with administrator privilege should rerun the command. There might be insufficient memory or disc capacity. Terminate unnecessary applications and rerun the setup command.

KNBB2712-E

An error occurred during removing CSA service. :*maintenance-information-1 maintenance-information-2 maintenance-information-3 maintenance-information-4*

An error occurred during the setup of the JP1/AJS3 for Cloud Service Applications service.

(S)

The system terminates the setup process.

(O)

Run the setup command as an OS user with Administrator privileges. There might be insufficient memory or disc capacity. Terminate unnecessary applications and rerun the setup command.

KNBB2714-E

Setup cannot be performed because the service (*service*) is active.

The service is running, so you cannot perform set up.

(S)

The system terminates the setup process.

(O)

Check if the JP1/AJS3 for Cloud Service Applications service is stopped.

KNBB2715-W

The command(*command*) ended warning.

The command (*command*) process has ended with warning.

(S)

The system outputs that to the log the command has been terminated with warning.

(O)

Before this message is displayed, the message indicating the cause of the warning is output to the command log. Investigate the cause according to the log immediately before this message and take action as necessary.

Note that the command may output this message and stop the JP1/AJS3 CSA Web Application Server service even though no error or warning message is output. In this case, there is no action required for this message. This message is generated because some internal processes were already stopped, and it indicates that the process of terminating the JP1/AJS3 CSA Web Application Server service has been completed normally.

(4) List of messages beginning with KNBB (messages about the web application server)

The following is a list of messages beginning with KNBB (messages about the web application server):

KNBB3001-I

The CSA Web Application Server service will now start.

This message reports that the startup process of the JP1/AJS3 CSA Web Application Server service has started.

(S)

The system has output to the log that the startup process of the JP1/AJS3 CSA Web Application Server service has started.

KNBB3002-I

The CSA Web Application Server service will now start.

This message reports that the JP1/AJS3 CSA Web Application Server service has been started.

(S)

The system has output to the log that the JP1/AJS3 CSA Web Application Server service has been started.

KNBB3003-E

An error occurred in the processing to start the CSA Web Application Server service.

This message reports that an error has occurred during the startup process of the JP1/AJS3 CSA Web Application Server service.

(S)

The system has output to the log that an error has occurred during the startup process of the JP1/AJS3 CSA Web Application Server service.

(O)

Before this message is displayed, the message indicating the error is output to the application server log. Take action according to the message that was output immediately before this message.

KNBB3004-E

An unexpected error occurred in the processing to start the CSA Web Application Server service.

An unexpected error occurred during the startup process of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process.

(O)

The configuration of JP1/AJS3 for Cloud Service Applications may be corrupt. Perform a recovery installation.

KNBB3005-I

The CSA Web Application Server service will now stop.

This message reports that the stop process of the JP1/AJS3 CSA Web Application Server service has started.

(S)

The system has output to the log that the JP1/AJS3 CSA Web Application Server service has been stopped.

KNBB3006-I

The CSA Web Application Server service stopped.

This message reports that the JP1/AJS3 CSA Web Application Server service has been stopped.

(S)

The system has output to the log that the JP1/AJS3 CSA Web Application Server service has been stopped.

KNBB3026-I

API processing will now start. (api type=*API-type*)

This message reports that the API process has started.

(S)

The system has output to the log that the API process has been started.

KNBB3027-I

API processing ended. (api type=*API-type*)

This message reports that the API process has completed.

(S)

The system has output to the log that the API process has been completed normally.

KNBB3028-E

An error occurred in the API processing. (api type=*API-type*)

This message reports that an error has occurred during the API process.

(S)

The system has output to the log that an error has occurred during the API process.

(O)

Take action according to the messages that were output before and after this message.

KNBB3029-I

exception-class-information

This message indicates where the exception occurred.

(S)

The system has output to the log an indication of the location where the exception occurred.

KNBB3030-I

stack-trace-information

This message shows the stack trace information.

The stack trace information is output according to the language type set in the OS.

(S)

The system has output the stack trace information to the log.

KNBB3031-I

API-input-information

This message shows the API input information.

(S)

The system has output the API input information to the log.

KNBB3033-I

API-execution-information

This message shows the API execution information.

(S)

The system has output the API execution information to the log.

KNBB3034-I

*UUID-set-by-the-service-linkage-job*Δ*JPI-user-name-when-the-job-is-run*Δ*agent-host-name*Δ*manager-host-name*Δ*scheduler-service-name*Δ*full-unit-name*Δ*execution-ID*Δ*job-ID* Δ*service-linkage-job-definition-name*Δ*authentication-definition-name*Δ*linkage-target-service-name*Δ*linkage-process-overview*Δ*command-line-of-execution-start-process*Δ*JPI-resource-group-name*

Legend:

Δ: Tab symbol

This message shows the information of the request source to get the information of the service linkage job.

(S)

The system has output the execution information of the service linkage job to the log.

KNBB3035-I

*UUID-set-by-the-service-linkage-monitoring-job*Δ*JPI-user-name-when-the-job-is-run*Δ*agent-host-name*Δ*manager-host-name*Δ*scheduler-service-name*Δ*unit-ID*Δ*execution-ID*Δ*service-linkage-monitoring-job-definition-name*Δ*authentication-definition-name*Δ*linkage-target-service-name*Δ*linkage-process-overview*Δ*command-line-of-execution-start-process*Δ*JPI-resource-group-name*Δ*initial-access-flag*

Legend:

Δ: Tab symbol

This message shows the information of the request source to get the information of the service linkage monitoring job.

(S)

The system has output the execution information of the service linkage monitoring job to the log.

KNBB3051-W

The file was not found. Processing will continue by using the default values. (file=*file-name*)

The file is not found.

(S)

The system assumes default value and continues processing.

KNBB3052-E

Failed to read the file. (file =*file-name*, maintenance information=*maintenance-information*)

An error occurred during the file input process for *file-name*. The following may be the cause.

- Unacceptable characters are specified for the file name or folder name.
- The length of the file name, folder name, or file path is incorrect.
- Insufficient capacity on the disc.
- Editing is in progress in another program.

(S)

The system aborts the process.

(O)

Eliminate the cause of errors and stop the JP1/AJS3 CSA HTTP Server service. Then, restart the JP1/AJS3 CSA Web Application Server service and start the JP1/AJS3 CSA HTTP Server service.

KNBB3054-E

An error occurred while the file was being accessed. (file =*file-name*, maintenance information=*maintenance-information*)

An error occurred during the file input process for *file-name*. The following may be the cause.

- Unacceptable characters are specified for the file name or folder name.
- The length of the file name, folder name, or file path is incorrect.
- There are no access rights for files and folders that store files.
- Insufficient capacity on the disc.
- Editing is in progress in another program.

(S)

The system aborts the process.

(O)

Eliminate the cause of errors and stop the JP1/AJS3 CSA HTTP Server service. Then, restart the JP1/AJS3 CSA Web Application Server service and start the JP1/AJS3 CSA HTTP Server service.

KNBB3056-E

The specified file is incorrect. (file = *file-name*, line=*line-number*)

The process was aborted because an incorrect specification was made in the file.

(S)

The system aborts the process.

(O)

Set the environment configuration file correctly. Change the settings and stop the JP1/AJS3 CSA HTTP Server service. Then, restart the JP1/AJS3 CSA Web Application Server service and start the JP1/AJS3 CSA HTTP Server service.

In *line-number*, the approximate location of the incorrect description will be output. If there is no error in *line-number*, review the descriptions before and after the *line-number*.

KNBB3059-I

configuration-definition-information

This message reports the configuration definition that has been loaded into memory.

(S)

The system has output the configuration definition that has been loaded into memory to the log.

KNBB3060-W

FILE RETRY WAITING ERR (maintenance information=*maintenance-information-1*, *maintenance-information-2*)

This message reports the failure to wait for file access retry.

(S)

The system has output to the log that there was a failure to wait for file access retry.

KNBB3061-W

FILE CLOSE ERR (maintenance information=*maintenance-information-1*, *maintenance-information-2*)

This message reports that the file close process failed.

(S)

The system has output to the log that the file close process has failed.

KNBB3062-I

The file (*file-name*) was read.

This message reports that the file has been read successfully.

(S)

The system has output to the log that the file has been loaded successfully.

KNBB3063-E

Failed to write the file. (file = *file-name*, maintenance information=*maintenance-information*)

An error occurred during the file output process for *file-name*. The following may be the cause.

- Unacceptable characters are specified for the file name or folder name.
- The length of the file name, folder name, or file path is incorrect.
- There are no access rights for files and folders that store files.
- Insufficient capacity on the disc.
- Editing is in progress in another program.

(S)

The system aborts the process.

(O)

Eliminate the cause of the error and try the operation again.

KNBB3064-I

The file was written. (file=*file-name*)

This message reports that the that the file has been written successfully.

(S)

The system has output to the log that the file was written successfully.

KNBB3102-E

The session that you are logged in to is no longer valid. Log in again.

The logged-in session is already invalid. Log in again.

(S)

The system aborts the process.

(O)

Log in again and try the operation again.

KNBB3103-W

The session that you are logged in to is no longer valid.

The logged-in session is already invalid.

(S)

The system has output to the log that the logged-in session is already invalid.

KNBB3104-I

Session created. (maintenance information=*maintenance-information*)

The logged-in session is already invalid.

(S)

The system has output to the log that a session has been created.

KNBB3105-I

The session timed out. (maintenance information=*maintenance-information*)

This message reports that a session timed out.

(S)

The system has output to the log that a session timed out.

KNBB3106-I

The session deleted. (maintenance information=*maintenance-information*)

This message reports that a session was deleted.

(S)

The system has output to the log that a session was deleted.

KNBB3151-E

The log output processing could not be initialized. (detailed information=*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4, detailed-information-5, detailed-information-6*)

An error occurred during the initialization of the log output process. The following may be the cause.

- The user does not have access privileges to the files at the lower level of the log folder.
- Insufficient capacity on the disc.

(S)

The system aborts the process.

(O)

Eliminate the cause of the error. If the problem cannot be solved, the configuration of JP1/AJS3 for Cloud Service Applications may be corrupt. Perform a recovery installation.

KNBB3152-W

The log could not be output. (detailed information=*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4, detailed-information-5, detailed-information-6, detailed-information-7*)

An error occurred during the log output process. The following may be the cause.

- The user does not have access privileges to the files at the lower level of the log folder.
- Insufficient capacity on the disc.

(S)

Continues processing.

(O)

Eliminate the cause of the error. If the problem cannot be solved, the configuration of JP1/AJS3 for Cloud Service Applications may be corrupt. Perform a recovery installation.

KNBB3153-W

Log output processing failed to complete. (detailed information=*detailed-information-1, detailed-information-2, detailed-information-3, detailed-information-4, detailed-information-5, detailed-information-6, detailed-information-7*)

An error occurred during the end processing of the log output process. The following may be the cause.

- The user does not have access privileges to the files at the lower level of the log folder.
- Insufficient capacity on the disc.

(S)

Continues processing.

(O)

Eliminate the cause of the error. If the problem cannot be solved, the configuration of JP1/AJS3 for Cloud Service Applications may be corrupt. Perform a recovery installation.

KNBB3208-E

The definition does not exist.

The definition does not exist.

(S)

Cancels processing.

(O)

The definition does not exist. Register it again.

KNBB3212-E

The user name or password is invalid.

Login failed because the JP1 username or password was invalid.

(S)

Cancels processing.

(O)

Enter the JP1 username and password registered on the Access Control Server to which it is connected and then log in.

KNBB3216-E

The request is incorrect.

The process was aborted because the request was incorrectly specified.

(S)

Cancels processing.

(O)

Use the data collection tool to collect data, and then contact the system administrator.

KNBB3238-E

The message body of the request is incorrect. (line=*line-number*)

There is an error in the description of the message body of the request.

(S)

Cancels processing.

(O)

Describe the message body of the request correctly.

In *line-number*, the approximate location of the incorrect description will be output. If there is no error in *line-number*, review the descriptions before and after the *line-number*.

KNBB3239-E

Specify a request header (*request-header*).

request-header is not specified.

(S)
Cancels processing.

(O)
Specify the *request-header*.

KNBB3240-E

The request header (*request-header*) is incorrect.

The value in *request-header* is incorrect.

(S)
Cancels processing.

(O)
Specify correct value for *request-header*.

KNBB3290-W

Failed to save the execution history. (*maintenance information=maintenance-information-1, maintenance-information-2*)

Failed to save execution history.

(S)
Continues processing.

KNBB3291-E

definition-type "definition-name" does not exist.

The specified definition name does not exist.

A *definition-type* displays one of the following:

- service linkage job definition
- service linkage monitoring job definition
- connection definition
- execution definition
- authentication definition
- monitoring definition

(S)
Cancels processing.

(O)
Refresh the web screen to confirm that the definition exists, and then select it again.

KNBB3609-E

An error occurred in the Access Control Server at the connection destination.
(maintenance information=*maintenance-information*)

Login or connection could not be established because an error occurred on JP1/Base at the connection destination during the user authentication process. The following may be the cause.

- The host name of the Access Control Server is incorrectly specified in the settings of JP1/Base at the connection destination.
- If the error message "KAVS1005-E Cannot connect to Access Control Server." is displayed in the Windows event log or syslog of the connection destination, the Access Control Server has not started.

(S)

Cancels processing.

(O)

Eliminate the cause of the error and try the operation again.

If the connection destination is UNIX and the Authorized Server is specified as local host, the settings for JP1/Base are required to start as the Access Control Server. For the setting method, see the description of specifying the Access Control Server in the *JP1/Base User's Guide*.

KNBB3669-E

The system could not connect to the Access Control Server at the connection destination.

Processing cannot start because the connection destination cannot connect to the Access Control Server.

(S)

Cancels processing.

(O)

Check whether the specified Access Control Server on JP1/Base at the connection destination is running or not.

KNBB3689-W

An attempt to release the login information failed. (maintenance information=*maintenance-information-1, maintenance-information-2*)

This message reports that the release process of login information failed.

(S)

The system has output to the log that the release process of login information failed.

KNBB3801-I

The database was backed up.

Backup of the database file has been completed.

(S)

Continues processing.

KNBB3802-W

An error occurred during backup of the database. (maintenance information=*maintenance-information*)

An error occurred during the database file backup.

The following factors may be the cause.

- The database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service.
- The database file has been destroyed.

(S)

Continues processing.

(O)

Check whether the database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service. If it is used by another process and this error message is not output at the next definition operation, no action is required. If this error message is output at the next definition operation, even if the database file is not used by other processes, restart the JP1/AJS3 CSA Web Application Server service. After the restart, if still this error message is output, collect the data and contact your system administrator.

KNBB3803-I

Database maintenance was performed.

Database maintenance has been completed.

(S)

Continues processing.

KNBB3804-W

An error occurred during maintenance of the database. (maintenance information=*maintenance-information*)

An error occurred during database maintenance.

The following factors may be the cause.

- The database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service.
- The database file has been destroyed.

(S)

Continues processing.

(O)

Check whether the database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service. If it is used by another process and this error message is not output at the next definition operation, no action is required. If this error message is output at the next definition operation, even if the database file is not used by other processes, restart the JP1/AJS3 CSA Web Application Server service. After the restart, if still this error message is output, collect the data and contact your system administrator.

KNBB3805-I

Maintenance of the execution history table was performed.

Maintenance of the execution history table has been completed.

(S)

Continues processing.

KNBB3806-W

An error occurred during maintenance of the execution history table. (maintenance information=*maintenance-information*)

An error occurred during maintenance of the execution history table.

The following factors may be the cause.

- The database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service.
- The database file has been destroyed.

(S)

Continues processing.

(O)

Check whether the database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service. If it is used by another process and this error message is not output at the next definition operation, no action is required. If this error message is output at the next definition operation, even if the database file is not used by other processes, restart the JP1/AJS3 CSA Web Application Server service. After the restart, if still this error message is output, collect the data and contact your system administrator.

KNBB3807-E

No authorization.

The operation-target definition does not have the required operation permissions.

(S)

The system aborts the process.

(O)

Review whether the JP1 user who is operating has the required operation permissions for the JP1 resource group name that is set in the operation-target definition. If the permissions are insufficient, grant the required privileges before starting the operation.

KNBB3808-E

An error occurred during the accessing of the database at the connection destination. (maintenance information=*maintenance-information*)

An error occurred during access to the database file.

The following factors may be the cause.

- The database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service.
- The database file has been destroyed.

(S)

The system aborts the process.

(O)

Check whether the database file is being used by a process other than the JP1/AJS3 CSA Web Application Server service. If it is being used by another process, check that the operation that caused this error is performed correctly after ending the process. If the operation is not performed correctly, try it again. If the same operation is performed again and the same error still occurs, restart the JP1/AJS3 CSA Web Application Server service. If the same error occurs even after restarting the JP1/AJS3 CSA Web Application Server service, restore the backed-up database file. If the same error occurs even after restoring the database file, collect the data and contact your system administrator.

KNBB3901-E

An unexpected error occurred during processing. (maintenance information=*maintenance-information-1, maintenance-information-2*)

An unexpected error occurred during processing. The following may be the cause.

- The configuration of JP1/AJS3 for Cloud Service Applications is corrupted.
- The API being processed was forcibly discarded because JP1/AJS3 for Cloud Service Applications was stopped or restarted.

(S)

The system aborts the process.

(O)

If the configuration of JP1/AJS3 for Cloud Service Applications has been changed, perform a recovery installation. If the JP1/AJS3 for Cloud Service Applications was stopped or restarted, check to what extent the API processing has been reflected.

Otherwise, eliminate the cause of the error. If the problem cannot be solved, collect the data and contact your system administrator.

KNBB3902-E

An system error occurred during processing. (maintenance information=*maintenance-information*)

A system error occurred during processing. There may be a problem with the execution environment of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process.

(O)

Eliminate the cause of the error. If the problem cannot be solved, collect the data and contact your system administrator.

KNBB3903-E

Memory became insufficient during processing. (maintenance information=*maintenance-information*)

Insufficient memory was detected in the execution environment of the JP1/AJS3 CSA Web Application Server service.

(S)

The system aborts the process.

(O)

Check the physical memory usage of the host where the JP1/AJS3 CSA Web Application Server service is running. If the capacity of the available physical memory is insufficient, terminate unnecessary applications to increase the size of available physical memory.

For details of required capacity of memory of JP1/AJS3 for Cloud Service Applications, see the *release notes*.

KNBB3905-E

An unexpected error occurred during processing. (maintenance information=*maintenance-information-1, maintenance-information-2*)

This message reports that an unexpected error has occurred during the process.

(S)

Continues processing.

(O)

The configuration of JP1/AJS3 for Cloud Service Applications may be corrupt. Perform a recovery installation. If the problem cannot be solved, collect the data and contact your system administrator.

(5) List of messages beginning with KNBB (messages about the Service linkage job definitions window)

The following is a list of messages beginning with KNBB (messages about the Service linkage job definitions window):

KNBB4000-W

The following items have been initialized due to an incorrect definition.

(Field name):

corresponding-field-name

corresponding-field-name

This message reports that there is an unacceptable input in *corresponding-field-name* because the job definition is invalid.

(S)

The system initializes the value in *corresponding-field-name*.

KNBB4001-E

Enter the correct value for (*field-name*).

The value was entered incorrectly in *field-name*.

(S)

The system aborts the process.

(O)

Re-enter the correct value in *field-name*.

KNBB4002-E

System error has occurred in the definition program. (func= *API-name*,err=*error-maintenance-information-*)

An unexpected error occurred during the definition program.

(S)

The system aborts the process.

(O)

This may be a temporary error. Close the Service Linkage Job Definition screen or the Service Linkage Monitoring Job Definition screen, and then reopen the screen to define the job.

If the same error occurs, the folder (*system-drive\temp*) required for the custom job definition linkage or custom event job definition linkage may be missing. See the description of the KAVV801-E message in the manual, *JP1/Automatic Job Management System 3 Messages* and take action. If the problem persists, collect the data by using the data collection tool and contact your system administrator.

KNBB4003-E

The *service-linkage-definition-information-file-name* could not be read correctly.

The *service-linkage-definition-information-file-name* could not be loaded correctly.

(The file may not exist, may not be opened, or the contents may be incorrect.)

A *service-linkage-definition-information-file-name* displays one of the following:

- service linkage definition information file
- service linkage monitoring definition information file

(S)

The system aborts the process.

(O)

Recreate the service linkage definition information file or the service linkage monitoring definition information file, and register the service linkage job or service linkage monitoring job again.

KNBB4004-E

Enter the (*field-name*).

No value was entered in *field-name*.

(S)

The system aborts the process.

(O)

Enter a value in *field-name*.

KNBB4009-E

Make sure that the total size of the input values for all items does not exceed *bytes* bytes.

The total size of the input value has exceeded the limit.

(S)

The system aborts the process.

(O)

Review the input values if there are any unnecessary values or values that can be shortened and click the **OK** button again.

KNBB4010-E

In *field-name*, enter values in *minimum-value* and *maximum-value*.

The *field-name* is outside the *minimum-value* - *maximum-value* range.

(S)

The system aborts the process.

(O)

Enter a value within the specifiable range.

KNBB4011-E

Specify the *field-name*.

The *field-name* is not specified.

(S)

The system aborts the process.

(O)

Specify the required item.

(6) List of messages beginning with KNBB (messages about the service linkage job definitions commands)

The following is a list of messages beginning with KNBB (messages about the service linkage job definitions commands).

KNBB4501-I

The *service-linkage-job-type* has been registered. (*service-linkage-job-name*)

The service linkage job or service linkage monitoring job is registered successfully.

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

KNBB4502-E

Specify the required option.

Required options are not specified.

(S)

The system aborts the process.

(O)

Specify required options and rerun the command.

KNBB4503-E

An invalid option is specified. (*option-name*)

You specified unavailable options.

(S)

The system aborts the process.

(O)

Specify the available option and rerun the command.

KNBB4504-E

Specify a value for the option. (*option-name*)

No value was specified for the option.

(S)

The system aborts the process.

(O)

Specify the value of the option and rerun the command.

KNBB4505-E

A value is specified for an option that does not require a value. (*option-name*)

A value has been specified for an option that does not require a value.

(S)

The system aborts the process.

(O)

Correct the command format and rerun the command.

KNBB4506-E

Specify the correct value for the option. (*option-name*)

The format of the option value is incorrect.

(S)

The system aborts the process.

(O)

Specify the correct value of the option and rerun the command.

KNBB4507-E

Option (*option-name*) appears twice or more.

The same option is specified twice or more.

(S)

The system aborts the process.

(O)

Correct the option specified twice or more to only once and rerun the command.

KNBB4508-E

job-name already exists.

You specified a custom job or a custom event job that already exists.

(S)

The system aborts the process.

(O)

Specify a job name that is not registered in JP1/AJS3 - View and rerun the command.

KNBB4509-E

The file could not be accessed. (*file-path-user-specified*)

You cannot access the specified file.

(S)

The system aborts the process.

(O)

Correct the access rights and existence of the file and rerun the command.

KNBB4511-E

The contents of service linkage definition information file are invalid. (*path-of-service-linkage-definition-information-file, detailed-information*)

The contents of the service linkage definition information file or service linkage monitoring definition information file are invalid.

The contents may have changed due to editing or saving the file using a text editor.

(S)

The system aborts the process.

(O)

Export the definition information file from JP1/AJS3 for Cloud Service Applications again and rerun the command.

KNBB4512-E

The *service-linkage-job-type* cannot be registered because the maximum number of *job-type* has been exceeded.

The maximum number of custom jobs or custom event jobs that View can hold has been exceeded.

A *job-type* displays one of the following:

- custom jobs
- custom event jobs

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

(S)

The system aborts the process.

(O)

Delete the unused custom job or custom event job and rerun the command, or register the jobs on another View host.

KNBB4513-E

You cannot execute a command while the Register Custom Job dialog box is open or the service linkage job operation command is being executed.

The command has run while the Register Custom Job screen was open or while the Import, List display, or Delete command is running.

(S)

The system aborts the process.

(O)

If the Register Custom Job dialog box is opened, close it and rerun the command.

If another service linkage job operation command is running, rerun the command after the operation command has completed.

KNBB4514-W

The *service-linkage-job-type* is not registered.

The service linkage job is not registered.

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

KNBB4515-I

The *service-linkage-job-type* has been deleted. (*deleted-service-linkage-job-name*)

The service linkage job was deleted successfully.

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

KNBB4516-E

Cannot specify these options together.

An option that cannot be specified at the same time has been specified.

(S)

The system aborts the process.

(O)

Check the specified option and rerun the command with a combination of options that can be specified at the same time.

KNBB4517-E

The specified *service-linkage-job-type* cannot be deleted because it does not exist. (*specified-job-name*)

You specified a service linkage job name that does not exist, or a custom job name other than a service linkage job.

Alternatively, you specified a service linkage monitoring job name that does not exist.

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

(S)

The system aborts the process.

(O)

Check the service linkage job name or the service linkage monitoring job name you want to delete and rerun the command.

KNBB4518-E

You cannot perform operations on *job-type* registration information.

A *job-type* displays one of the following:

- custom job
- custom event job

If the *job-type* is a custom job, operations cannot be performed for the following reasons:

- Read and write permissions are not set for files located under the custom job registration information folder^{#1}.
- Files located under the custom job registration information folder^{#1} are being edited in another program.

If the *job-type* is a custom event job, operations cannot be performed for the following reasons:

- Read and write permissions are not set for files located under the custom event job registration information folder^{#2}.
- Files located under the custom event job registration information folder^{#2} are being edited in another program.

#1:

The following folder:

View_Data_Path^{#3}\custom.dir\

#2:

The following folder:

View_Data_Path^{#3}\customevent.dir\

#3:

View_Data_Path: JP1/AJS3 - View data folder

(S)

The system aborts the process.

(O)

Eliminate the cause of the error.

KNBB4519-E

You cannot perform operations on *service-linkage-job-type*-specific information.

A *service-linkage-job-type* displays one of the following:

- service linkage job
- service linkage monitoring job

If the *service-linkage-job-type* is a service linkage job, operations cannot be performed for the following reasons:

- Read and write permissions are not set for the service linkage job-specific information storage destination folder^{#1} and files located under the folder.
- Files located under the service linkage job-specific information storage destination folder^{#1} are being edited in another program.

If the *service-linkage-job-type* is a service linkage monitoring job, operations cannot be performed for the following reasons:

- Read and write permissions are not set for the service linkage monitoring job-specific information storage destination folder^{#2} and files located under the folder.
- Files located under the service linkage monitoring job-specific information storage destination folder^{#2} are being edited in another program.

#1:

Either of the following folders:

- *View_Path*^{#3}\image\custom
- *View_Data_Path*^{#4}\csadef

#2:

Either of the following folders:

- *View_Path*^{#3}\image\custom
- *View_Data_Path*^{#4}\csadef\evcustom

#3:

View_Path: JP1/AJS3 - View installation folder

#4:

View_Data_Path: JP1/AJS3 - View data folder

(S)

The system aborts the process.

(O)

Eliminate the cause of the error.

KNBB4520-E

A system error occurred in the service linkage job operation command. (func = *API name*, err = *error-maintenance-information*)

An unexpected error occurred during the service linkage job or service linkage monitoring job operation command.

(S)

The system aborts the process.

(O)

Collect the data by using the data collection tool and contact your system administrator.

KNBB4521-E

Failed to initialize log output processing. (*detailed-information-1*, *detailed-information-2*)

An error occurred during the initialization of the log output process.

(S)

The system aborts the process.

(O)

The user does not have access privileges to the files at the lower level of the log folder or there might be insufficient memory or disc capacity.

Eliminate the cause of the error. If the problem cannot be solved, the configuration of JP1/AJS3 - View may be corrupted. Perform a recovery installation.

KNBB4522-E

Failed to output log information. (*detailed-information-1*, *detailed-information-2*)

An error occurred during the log output process. The following may be the cause.

- The user does not have access privileges to the files at the lower level of the log folder.
- Insufficient capacity on the disc.

The location of the log folder is as follows:

%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1AJS2V\log

The default for %ALLUSERSPROFILE% is *system-drive*\ProgramData.

(S)

The system aborts the process.

(O)

Eliminate the cause of the error.

KNBB4523-E

An unexpected error occurred during the startup process. (Detailed information: *maintenance-information-1, maintenance-information-2*)

An unexpected error occurred during the start processing of service linkage job or service linkage monitoring job operation command.

(S)

The system aborts the process.

(O)

There might be insufficient memory or disc capacity. Terminate unnecessary applications and rerun the command. If the problem cannot be solved, the configuration of JP1/AJS3 - View may be corrupted. Perform a recovery installation.

KNBB4524-E

Failed to start the service linkage job operation command. (Detailed information: *maintenance-information*)

The system failed to start the service linkage job or service linkage monitoring job command.

(S)

The system aborts the process.

(O)

The following factors may be the cause.

- There might be insufficient memory or disc capacity. Terminate unnecessary applications and rerun the command.
- JP1/AJS3 - View is installed in the root of the drive. Install JP1/AJS3 - View in a location other than the root of the drive.

If the problem cannot be solved, the configuration of JP1/AJS3 - View may be corrupted. Perform a recovery installation.

KNBB4525-E

No authority to execute the service linkage job operation command.

The user who tried to run the service linkage job or service linkage monitoring job operation command does not have the required command operation permissions.

(S)

The system aborts the process.

(O)

Rerun the command on a command prompt running with administrator privileges.

KNBB4526-W

The folder specified in the environment variable *environment-variable-name* does not exist. The default folder will be used.

The folder specified in the environment variable does not exist.

Use the default custom job or custom event job registration information folder^{#1} and folder^{#2} containing the service linkage job or service linkage monitoring job-specific information.

#1:

View_Data_Path^{#3}\custom.dir (for a service linkage job)

View_Data_Path^{#3}\customevent.dir (for a service linkage monitoring job)

#2:

View_Data_Path^{#3}\csadef (for a service linkage job)

View_Data_Path^{#3}\csadef\customevent (for a service linkage monitoring job)

#3:

View_Data_Path: JP1/AJS3 - View data folder

An *environment-variable-name* displays one of the following:

- AJS_CSA_VIEW_CUSTOMJOBDIR
- AJS_CSA_VIEW_CUSTOMEVJOBDIR

KNBB4527-E

custom-job-name cannot be registered because a custom job other than a service linkage job of the same name exists.

Forced overwrite option was specified for a custom job other than a service linkage job.

(S)

The system aborts the process.

(O)

Specify another custom job name and rerun the registration command.

KNBB4528-E

The command line parameter is too long.

The command line parameters specified for the command are too long. The command cannot be started.

(S)

Cancels processing.

(O)

Correctly specify the command line parameters, and then re-execute the command.

(7) List of messages beginning with KNBB (messages about the service linkage job execution programs)

The following is a list of messages beginning with KNBB (messages about the service linkage job execution programs).

KNBB6000-I

The service linkage job will now start.

The service linkage job will be started.

(S)

Continues processing.

KNBB6001-I

The service linkage job will now end.

The service linkage job will be ended.

(S)

Continues processing.

KNBB6002-I

Communication with the CSA server will now start.

The communication with the JP1/AJS3 for Cloud Service Applications server will be started.

(S)

Continues processing.

KNBB6003-I

Communication with the CSA server ended.

The communication with the JP1/AJS3 for Cloud Service Applications server ends.

(S)

Continues processing.

KNBB6004-I

process-name

This message reports the name and command line of the process to be executed from now.

The command line for the processing name will be output in the next line with the same process ID and same thread ID.

(S)

Continues processing.

KNBB6005-I

The service linkage objects monitoring job will be started. (*monitoring-target-file-name*)

The service linkage objects monitoring job will be started.

The system starts monitoring the monitoring target file.

(S)

Continues processing.

KNBB6011-I

The service linkage objects monitoring process will be started.

The service linkage objects monitoring process will be started.

(S)

The system starts the service linkage objects monitoring process.

KNBB6012-I

The service linkage objects monitoring process will be terminated.

The service linkage objects monitoring process will be terminated.

(S)

The system terminates the service linkage objects monitoring process.

KNBB6013-I

The object (*object-name*) has been created.

The object was created.

(S)

Continues processing.

KNBB6014-I

The object (*object-name*) existed when the job was started.

The object existed when the job was started.

(S)

Continues processing.

KNBB6015-I

The object (*object-name*) has been deleted.

The object was deleted.

(S)

Continues processing.

KNBB6016-I

No objects existed when the job was started.

No objects existed when the job was started.

(S)

Continues processing.

KNBB6017-I

The object (*object-name*) has been updated.

The object was updated.

(S)

Continues processing.

KNBB6018-W

The time-out period elapsed.

The time-out period has elapsed. The job will be terminated.

(S)

The job is timed-out and terminated based on the time-out period specified.

KNBB6100-E

The acquired value is incorrect. (*maintenance-information*)

An environment variable or CSA definition item has an error in one of the following:

- Required value has no value
- Character count
- Format (character string, numeric, etc.)

The environment variable name or maintenance information is output in Maintenance information.

(S)

The system aborts the process.

(O)

Specify the following values correctly and then rerun the command.

- Environment variable
 - AJS_CSA_AUTHINFNAME
 - AJS_CSA_DEFINFNAME
 - AJS_CSA_ENV_ *variable-value*
- CSA definition

KNBB6101-E

The environmental setting parameter is invalid. (*parameter-name*)

The specification of environment setting parameter is invalid.

(S)

The system aborts the process.

(O)

Redefine the environment definition as necessary.

KNBB6102-E

The job definition is incorrect. (*key-name*)

The job definition contains one of the following errors:

- Required values not entered
- Character length
- Format (character string, numerals, etc.)

(S)

The system aborts the process.

(O)

Define the correct job, and then rerun the process.

KNBB6103-E

The definition of the service linkage monitoring job does not match the definition on the CSA server.

The definition of the service linkage monitoring job does not match the monitoring definition on the JP1/AJS3 for Cloud Service Applications server.

The following factors may be the cause.

On update is specified as the job definition monitoring condition, but no update monitoring target is specified for the monitoring definition on the JP1/AJS3 for Cloud Service Applications server.

(S)

The system aborts the process.

(O)

Specify an update monitoring target for the monitoring definition on the JP1/AJS3 for Cloud Service Applications server, and then rerun the service linkage monitoring job.

KNBB6104-W

A macro variable exceeds 4096 bytes.

A macro variable exceeded 4,096 bytes after conversion.

(S)

The maximum size of a macro variable is 4,096 bytes. If a macro variable exceeds 4,096 bytes, any excessive information is truncated and the process continues.

(O)

Data exceeding 4,096 bytes in a macro variable is not passed onto succeeding jobnets or jobs. Check the execution status of any succeeding jobnet or job, and review the job definition if problems are found.

KNBB6105-E

An error occurred during extraction from the object list information. (*maintenance-information-1, maintenance-information-2*)

An error occurred when extracting information from the object list information based on the extraction position information.

(S)

The system aborts the process.

(O)

Confirm the following:

- Whether the object list information was properly acquired
- Whether the results obtained from object list information are in the expected format
- Whether the correct extraction position information was specified
- Whether the memory is enough

If there is not enough memory, check whether the output amount of the execution results (standard output) of the command executed from the service linkage monitoring job is large. If the output amount is large, adjust the options of the command to be executed from the service linkage monitoring job so that unnecessary information is not output.

KNBB6106-E

The result of extraction from the object list information is incorrect. (*maintenance-information-1, maintenance-information-2*)

The result of extraction from the object list information is incorrect.

(S)

The system aborts the process.

(O)

The following factors may be the cause, depending on the *maintenance-information-1* value.

Review the command execution result and extraction position information.

- When 1
The result of applying the extraction position information to the object list information result is in the incorrect JSON format.
- When 2
The result of applying the extraction position information to the object list information result is not in JSON array format.
- When 3
The object name extraction result is not a JSON array with string elements.

- When 4
The extraction results for the specified update monitoring targets 1 to 3 contain elements other than string values, numerical values, Boolean values, and null values.
- When 5
The number of elements in the object name extraction result does not match the number of elements in the extract result for the specified update monitoring targets 1 to 3.
- When 6
The result of extraction from the object name is a null character.

KNBB6107-E

Numerical information has been detected that cannot be handled by service linkage objects monitoring job. (*maintenance-information*)

Numerical information extracted from the extraction position information in the update monitoring target information contained numerical values that cannot be handled by the service linkage objects monitoring job.

(S)

The system aborts the process.

(O)

Numerical information that can be handled by update monitoring target information in the service linkage objects monitoring job includes the following:

Integers from -10,995,116,277,760 to 10,995,116,277,760

When handling numerical information, truncate the information to fit within this value range, and then rerun the service linkage objects monitoring job.

KNBB6150-E

The service linkage objects monitoring process will be terminated. (*maintenance-information*)

An error has been detected with the service linkage objects monitoring process, and it will be terminated.

(S)

A non-continuable error occurred during processing, terminating the service linkage objects monitoring process. The service linkage objects monitoring job cannot perform monitoring.

KNBB6151-W

The memory for message output became insufficient. (*manager-host-name, scheduler-service-name, unit-ID, execution-ID, maintenance-information*)

Out of memory has occurred. Messages cannot be output to detailed execution results.

(S)

Out of memory has occurred. The process will continue without outputting messages to detailed execution results.

(O)

Check that there is sufficient memory.

For details about the memory requirements for JP1/AJS3, see the description of the required memory size and disk utilization in the *Release Notes*.

KNBB6152-E

Memory became insufficient. (*maintenance-information*)

Out of memory has occurred.

(S)

The system checks whether the object status has been updated again at the next monitoring interval. Alternatively, the corresponding job ends abnormally.

(O)

Check whether you have sufficient memory to execute the program. Check whether any service linkage objects monitoring jobs have ended abnormally using JP1/AJS3 - View. If service linkage objects monitoring jobs have ended abnormally, register them again.

KNBB6153-E

The service linkage objects monitoring process could not be started. (*maintenance-information*)(*maintenance-information*)

The service linkage objects monitoring process failed to start.

(S)

A non-continuable error occurred during the service linkage objects monitoring job process startup process, terminating the process. The service linkage objects monitoring job cannot perform monitoring.

(O)

Check whether a resource shortage has occurred. After confirming, restart JP1/AJS3.

KNBB6154-E

An attempt to obtain pipe data failed. (*maintenance-information*)(*maintenance-information*)

An error occurred in inter-process communication with the agent, and the service linkage objects monitoring process will be terminated.

(S)

An error occurred in inter-process communication with the agent, and the service linkage objects monitoring process will be terminated. The service linkage objects monitoring job cannot perform monitoring.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

After confirming, restart JP1/AJS3.

KNBB6155-E

An attempt to send pipe data failed. (*maintenance-information*)(*maintenance-information*)

Inter-process communication with the agent failed.

(S)

An error occurred in inter-process communication with the agent. Depending on the location where the error occurred, the service linkage objects monitoring process will be terminated. In such cases, the service linkage objects monitoring job cannot perform monitoring. Service linkage objects monitoring job event detection may have failed.

(O)

Check whether system resources are sufficient, or whether the directory created when installing JP1/AJS3 has been accidentally deleted. If the service linkage objects monitoring process is running, check the service linkage objects monitoring job that returned an error in JP1/AJS3 - View, and rerun the job. If the service linkage objects monitoring process is stopped, restart JP1/AJS3.

KNBB6156-E

An error occurred during the operation of a file. (*maintenance-information*)(*maintenance-information*)

Failed to open the information file handled by the service linkage objects monitoring process.

(S)

The monitoring start process for the corresponding job cannot be executed.

(O)

Check whether system resources are sufficient, or whether the directory created when installing JP1/AJS3 has been accidentally deleted.

After confirming, check the service linkage objects monitoring job that returned an error in JP1/AJS3 - View, and rerun the job.

KNBB6157-E

The initialization of communication with the `jpoagtjobshow` command failed. (*return-code*)(*line-number*)

Failed the required initialization process to communicate with the `jpoagtjobshow` command.

(S)

Continues processing. However, information is not provided to the `jpoagtjobshow` command.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

To display the correct information with the `jpoagtjobshow` command, restart JP1/AJS3.

KNBB6158-E

The reading of requests from the `jpoagtjobshow` command failed. (*return-code*)

Failed to read from the pipe of the `jpoagtjobshow` command.

(S)

Continues processing. However, information is not provided to the `jpoagtjobshow` command.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

To display the correct information with the `jpoagtjobshow` command, rerun the command.

KNBB6159-E

The creation of information sent to the `jpoagtjobshow` command failed. *(return-code)(line-number)*

Failed to create an information file for the `jpoagtjobshow` command.

(S) Continues processing. However, information is not provided to the `jpoagtjobshow` command.

(O) Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

To display the correct information with the `jpoagtjobshow` command, rerun the command.

KNBB6160-E

The reporting of information to the `jpoagtjobshow` command failed. *(return-code)*

Failed to write to the pipe of the `jpoagtjobshow` command.

(S) Continues processing. However, information is not provided to the `jpoagtjobshow` command.

(O) Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

To display the correct information with the `jpoagtjobshow` command, rerun the command.

KNBB6161-E

The creation of the information to be sent to the `jpoagtjobshow` command is incomplete. *(return-code)(line-number)*

There is job information that could not be written when creating the information file for the `jpoagtjobshow` command.

(S) Continues processing. However, information is not provided to the `jpoagtjobshow` command.

(O) Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

To display the correct information with the `jpoagtjobshow` command, rerun the command.

KNBB6162-W

The status passing option file cannot be opened. The status passing cannot be executed. (*manager-host-name, scheduler-service-name, unit-ID, execution-ID, maintenance-information*)

The status passing information storage file cannot be opened for the service linkage objects monitoring job. The object monitoring status is not passed on. When JP1/AJS3 is started, processing is performed without the status of objects monitored when the service stopped being passed on.

(S)

The object monitoring status is not passed on. When JP1/AJS3 is started, service linkage objects monitoring job processing is performed without the status of objects monitored when the service stopped being passed on.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.
- For cluster operation, whether operating settings in FQDN format are the same for primary and secondary nodes when operating a DNS using a service linkage objects monitoring job.

KNBB6163-E

An attempt to set the next time monitoring failed. (*maintenance-information*)(*maintenance-information*)

Failed to configure settings for the next monitoring process.

(S)

An error occurred in the settings for the next monitoring process. The system checks whether the object status has been updated again at the next monitoring interval. Alternatively, the corresponding job ends abnormally.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

KNBB6164-E

The job could not be started. (*maintenance-information*)(*maintenance-information*)

Failed to start the job.

(S)

An error occurred in the job startup process. The corresponding job will end abnormally.

(O)

Confirm the following:

- Whether system resources are sufficient.
- Whether the permissions environment for the startup user is correct.
- Whether the directory created when installing JP1/AJS3 has been accidentally deleted.

KNBB6200-E

Failed to read the connection configuration file. (*connection-configuration-file-name*)

The loading of the connection configuration file of the service linkage job or service linkage monitoring job failed.

(S)

The system aborts the process.

(O)

Check the following possible causes.

1. There is no connection configuration file.
2. The path to the connection configuration file is incorrect.
3. You do not have permission to access the connection configuration file.

Take the following actions and try again.

1. Set the connect configuration file.
2. Enter the correct path to the connect configuration file.
3. Set access privileges to the connection configuration file.

KNBB6201-E

The syntax of the connection configuration file is incorrect. (*maintenance-information-1, maintenance-information-2*)

There is an error in the syntax of connection configuration file for the service linkage job or service linkage monitoring job.

The following factors may be the cause.

- A value is not specified.
- The length of the value is invalid.
- The value is not one of the available values.
- Out of the range of available values.
- Required specifications are not satisfied.
- Unknown item name is specified.

(S)

The system aborts the process.

(O)

Correct the connection configuration file and try again.

KNBB6202-E

An error occurred during communication with the CSA server. (*maintenance-information*)

An error occurred during the communication with the JP1/AJS3 for Cloud Service Applications server.

The following causes for the job execution host can be considered.

- The settings of connection configuration file are incorrect.
- The environment is not capable of communicating with the JP1/AJS3 for Cloud Service Applications server.
- JP1/AJS3 for Cloud Service Applications server host and JP1/AJS3 for CSA are stopped.
- A network failure has occurred.
- The SSL communication settings do not match the JP1/AJS3 for Cloud Service Applications server.

(S)

The system aborts the process.

(O)

Eliminate the cause of the error and try again.

- CSAServerName
- CSAConnectProtocol
- CSAConnectPortNumber
- ProxyAddr
- CAFile

If the problem cannot be solved, collect the data by using the data collection tool and contact your system administrator.

KNBB6203-E

An error occurred on the CSA server. (*maintenance-information*)

An error occurred on the JP1/AJS3 for Cloud Service Applications server.

The probable causes are as follows:

- The connection configuration file for the job execution host is configured incorrectly.
- The user does not have permission for the definitions on the JP1/AJS3 for Cloud Service Applications server.
- The definition does not exist on the JP1/AJS3 for Cloud Service Applications server.

(S)

The system aborts the process.

(O)

Confirm the JP1/AJS3 for Cloud Service Applications message.

Additionally, confirm whether the following are correct, and specify the correct values.

- The ProxyAddr setting specified in the connection configuration file
- The definitions name specified in JP1/AJS3 for Cloud Service Applications for the service linkage job definition or the service linkage monitoring job definition

- The JP1 user name used when executing the service linkage job or the service linkage monitoring job, and the permissions level in JP1/AJS3 for Cloud Service Applications set for the JP1 user name
- The resource group name for the definition in JP1/AJS3 for Cloud Service Applications

KNBB6204-E

The host name of the CSA server (*JP1/AJS3 for Cloud Service Applications-server-name*) cannot be resolved. (*agent-host-name*)

The IP address could not be resolved from the host name *JP1/AJS3 for Cloud Service Applications-server-name* of the JP1/AJS3 for Cloud Service Applications server.

(S)

The system aborts the process.

(O)

On *agent-host-name*, in order to resolve the IP address of the host name *JP1/AJS3 for Cloud Service Applications-server-name* of the JP1/AJS3 for Cloud Service Applications server, correct the settings of the `hosts` file, `jp1hosts` file, `jp1hosts2` file, or DNS. Then, confirm that the IP address of the host name of JP1/AJS3 for Cloud Service Applications server is set correctly. After that, try again.

If the above measures do not solve the problem, collect the data by using the data collection tool and contact your system administrator.

KNBB6205-W

An attempt to communicate with the CSA server will be retried because an error occurred during communication with the CSA server. (*maintenance-information*)

An error occurred during the communication with the JP1/AJS3 for Cloud Service Applications server. Retry the request to the JP1/AJS3 for Cloud Service Applications server according to the settings for retry interval and retry count. After this message is output, wait for the retry interval and then retry. If an error occurs even after reaching the maximum retry count, the KABB6202-E message will be output.

(S)

Continues processing.

(O)

Check whether the JP1/AJS3 for Cloud Service Applications server host and JP1/AJS3 for Cloud Service Applications are running.

KNBB6300-E

The format of the information obtained from CSA is invalid. (*host-name-of-connect-target-JP1/AJS3 for Cloud Service Applications, port-number-of-connect-target-JP1/AJS3 for Cloud Service Applications*)

The format of the information obtained from JP1/AJS3 for Cloud Service Applications is invalid. The information may be corrupted due to a communication problem with JP1/AJS3 for Cloud Service Applications.

(S)

The system aborts the process.

(O)

Check whether the host name and port number of the JP1/AJS3 for Cloud Service Applications at the connection destination are correct.

If the problem cannot be solved, collect the following data and contact your system administrator.

- Log information of the JP1/AJS3 for Cloud Service Applications at the connection destination
- Log information of the host where the job is executed

KNBB6301-E

The command executed from the service linkage job ended abnormally. (*process-name, return-value-of-command-executed-from-service-linkage-job, maintenance-information*)

The command executed by the service linkage job ended abnormally.

(S)

The system aborts the process when an error occurred during the connection processing. If an error occurred in a command executed by a subsequent service linkage job, then the system continues the job output and subsequent processes.

(O)

Check the following and try again.

- If KNBB6004-I was output immediately before, there is no error in the command executed by the service linkage job.
- The input information of the command executed by the service linkage job is appropriate.
- The abnormal end setting is as designed.

KNBB6302-E

The job will end abnormally because it did not meet the defined conditions. (*process-name, value-of-variable-specified-in-the-processing-condition*)

The job will be end abnormally if either of the following conditions did not match.

- The value of the variable specified for the process normal end condition and the value of the process normal end condition
- The value of the variable specified for the process continuation condition, and both of the value of the process normal end condition and the value of the retry condition for the process continuation condition

(S)

The system continues the job output and subsequent processes.

(O)

The service executed by the cloud service may be in an abnormal state. Check the status and eliminate the cause.

KNBB6303-E

The number of repetitions specified in the continuation condition has been exceeded. (*process-name, value-of-variable-specified-in-the-processing-condition*)

The process exceeded the number of repeat count specified in the continuation condition.

(S)

The system continues the job output and subsequent processes.

(O)

The service executed by the cloud service may be in an abnormal state. Check the status and eliminate the cause.

KNBB6304-E

Failed to execute the command from the service linkage job. (*maintenance-information*)

The command could not run from the service linkage job.

The OS environment might not be configured correctly (for example, the PATH environment variable is specified incorrectly).

(S)

The system aborts the process.

(O)

Check that the OS environment is configured correctly (for example, whether the PATH environment variable is specified incorrectly by the job execution host).

If you cannot solve the problem, use the data collection tool to collect data, and then contact the system administrator.

KNBB6305-E

The command executed from the service linkage job was ended by a signal. (*maintenance-information*)

The command run by a service linkage job was terminated because of a signal.

(S)

The system aborts the process when an error occurred during the connection processing. If an error occurred in a command executed by a subsequent service linkage job, then the system continues the job output and subsequent processes.

(O)

Check whether the command run by the service linkage job was not terminated forcibly.

KNBB6306-E

The standard output from the command executed by the service linkage objects monitoring job has exceeded the maximum. (*maintenance-information*)

The standard output from the command executed by the service linkage objects monitoring job for object monitoring has exceeded the `LimitObjMonStdOutSize` environment setting parameter.

The following may have occurred.

- The command line specified in the monitoring definition on the JP1/AJS3 for Cloud Service Applications server contains errors.
- There are too many objects or information to acquire.

(S)

The connection termination processing is executed if it is configured. The job will end abnormally.

(O)

Check for errors in the command line defined for the monitoring definition on the JP1/AJS3 for Cloud Service Applications server.

Either edit the command line, or reduce the number of objects to limit the number of objects or information acquired as a result of running the command.

KNBB6307-W

The standard error output from the command executed by the service linkage objects monitoring job has exceeded the maximum. (*maintenance-information*)

The standard error output from the command executed by the service linkage objects monitoring job for object monitoring exceeded 3,072KB.

When the standard error output from the command executed is specified in the monitoring definition on the JP1/AJS3 for CSA server to output to a log or detailed execution results, the information may get cut off, or become garbled.

The following factors may be the cause.

The command line specified in the monitoring definition for JP1/AJS3 for CSA at the connection destination contains errors.

(S)

Continues processing.

(O)

Check for errors in the command line defined for the monitoring definition on the JP1/AJS3 for Cloud Service Applications server, and then apply countermeasures.

KNBB6308-W

The command executed by the service linkage objects monitoring job has been terminated abnormally, but the monitoring will continue in accordance with the monitoring definition.

The command executed by the service linkage monitoring job has been terminated abnormally. Monitoring will continue in accordance with the monitoring definition.

(S)

Continues processing.

(O)

Confirm the following:

- If KNBB6004-I is output immediately before, check whether the command executed from the service linkage monitoring job contains errors.
- Whether the input information of the command executed from the service linkage monitoring job is correct.
- Whether the abnormal end settings are as intended.

KNBB6309-E

The user could not be masked. (*agent-host-name, manager-host-name, JP1-user-name*)

Failed to mask user when executing commands in the service linkage monitoring job.

(S)

The system aborts the process.

(O)

Check the following possible causes.

1. The manager host name specified as the server host name for the JP1 user is incorrect on the agent host.
2. The JP1 user is not registered in the user mapping definition on the agent host.
3. A non-existent OS user is registered in the user mapping definition on the agent host.
4. The wrong OS user password is registered in the user mapping definition on the agent host (Windows only).
5. There is no JP1 user with the same name as the OS user that executed the `aj Sentry` command.
6. The owner JP1 user is different to the JP1 user responsible for execution registration.
7. Out of memory has occurred.
8. If **Owner user** is specified as the **Executed by** in the detailed definition of the job, and the **Owner** field is blank, an OS user with a name not registered as a JP1 user is set as the account under which the JP1/AJS3 service is activated on the manager host.

After addressing the potential factors, reissue the request.

1. Set the correct manager host name as the server host name for the JP1 user.
2. In the user mapping definition for the agent host executing the job, register the JP1 user displayed as the *JP1-user-name* in the message and map it to the OS user.
3. In the user mapping definition for the agent host executing the job, register an OS user that exists.
4. Run the `jbsumappass` command and set the password for the OS user again. Specify the OS user password as the password. (Windows only)
5. After performing either of the following actions, rerun the `aj Sentry` command.
 - Add a JP1 user with the same name as the OS user, and map the JP1 user with the OS user.
 - In the job definition, specify the owner as the user executing the job.
6. Determine whether to register job execution as the owner or as the user performing an execution registration, and correctly configure the **Executed by**.
7. Confirm the memory status, and review the expected memory requirements.
8. In the user mapping definition, register the JP1 user displayed as the *JP1-user-name* in the message. When using Windows, set an OS user of the same name as the user name registered as the JP1 user on the startup account for the JP1/AJS3 service on the manager host.

For details about how to configure user mapping settings, see 3. *Setup* in the manual *JP1/Automatic Job Management System 3 Configuration Guide* (for Windows), or 13. *Setup* in the manual *JP1/Automatic Job Management System 3 Configuration Guide* (for UNIX).

For details about JP1/AJS3 commands, see 3. *Commands Used for Normal Operations* in the manual *JP1/Automatic Job Management System 3 Command Reference*, or 4. *Commands Used for Special Operations* in the manual *JP1/Automatic Job Management System 3 Command Reference*.

For details about JP1/Base commands, see the manual *JP1/Base User's Guide*.

KNBB6310-E

The command executed from the service linkage monitoring job ended abnormally. (*process-name, return-code-for-command-executed-from-service-linkage-monitoring-job, maintenance-information*)

The command executed from the service linkage monitoring job ended abnormally.

(S)

The system aborts the process when an error occurred during connection processing.

If an error occurred in a command executed during monitoring processing, the process will continue from connection termination processing.

(O)

Check the following and try again.

- There is no error in the command executed by the service linkage monitoring job.
- The input information of the command executed by the service linkage monitoring job is appropriate.
- The abnormal end setting is as designed.

KNBB6311-E

Failed to execute the command from the service linkage monitoring job. (*maintenance-information*)

The command could not run from the service linkage monitoring job.

The OS environment might not be configured correctly (for example, the `PATH` environment variable is specified incorrectly).

(S)

The system aborts the process.

(O)

Check that the OS environment is configured correctly (for example, whether the `PATH` environment variable is specified incorrectly by the job execution host).

If you cannot solve the problem, use the data collection tool to collect data, and then contact the system administrator.

KNBB6312-E

The command executed from the service linkage monitoring job was ended by a signal. (*maintenance-information*)

The command run by a service linkage monitoring job was terminated because of a signal.

(S)

The system aborts the process when an error occurred during the connection processing.

If an error occurred in a command executed by a monitoring process, then the system continues processing from connection termination processing.

(O)

Check whether the command run by the service linkage monitoring job was not terminated forcibly.

KNBB6400-E

Failed to acquire an environment variable. (*environment-variable-name, maintenance-information-1, maintenance-information-2*)

The acquisition of the environment variable failed.

(S)

The system aborts the process.

- (O)
- Check whether the length of the value of environment variable specified for the variable is not too long.
If the problem cannot be solved, collect the data by using the data collection tool and contact your system administrator.

KNBB6401-E

An attempt to obtain the environment-setting-parameter (*environment-setting-parameter*) failed. (*logical-host-name*)

The system failed to acquire the environment setting parameter. For physical host, JP1_DEFAULT is output to *logical-host-name*.

- (S)
- The system aborts the process.
- (O)
- Set the value output to the *environment-setting-parameter* correctly in the environment where the job is executed.
For the output item name, see the manual.

KNBB6402-E

The service linkage objects monitoring thread has been terminated abnormally. (*maintenance-information*)

The system abnormally terminated the thread for monitoring objects in the service linkage objects monitoring job.

- (S)
- The system terminates the service linkage objects monitoring process.
- (O)
- An excessive load may have been applied to the CPU. Check the CPU load.
If you cannot solve the problem, use the data collection tool to collect data, and then contact the system administrator.

KNBB6403-W

The status passing information file is in an invalid format, so the status will not be passed. (*manager-host-name, scheduler-service-name, unit-ID, execution-ID, maintenance-information*)

The format of the status passing information storage file in the service linkage objects monitoring job is incorrect. The object monitoring status is not passed on. When JP1/AJS3 is started, processing is performed without the status of objects monitored when the service stopped being passed on.

- (S)
- The object monitoring status is not passed on. When JP1/AJS3 is started, service linkage objects monitoring job processing is performed without the status of objects monitored when the service stopped being passed on.
- (O)
- Confirm the following:
- Whether JP1/AJS3 inappropriately manipulates directories and files created upon installation.

KNBB6449-E

Writing to the file failed. (*file-name*)

Failed to write to the file.

(S)

The system aborts the process.

(O)

The possible reasons are shown below. Please verify and address these.

- The file path is long.
- No access permission is assigned to the folder.
- No upper-level folder exists. Alternatively, no access permission is assigned.
- Free disk space is running short.
- Another program is accessing the folder.
- System resources are running short.

If the problem persists, collect information by using the information collection tool and contact the system administrator.

KNBB6450-E

Memory became insufficient. (*maintenance-information*)

Out of memory has occurred.

(S)

The system aborts the process.

(O)

Check the output volume of the execution results (standard output, standard error output) of the command run by the service linkage job and service linkage monitoring job. If the volume of output is too great, adjust it with the options of the command executed by the service linkage job and service linkage monitoring job so that unnecessary information is not output.

In other cases, see 3. *Estimates* in the *JP1/Automatic Job Management System 3 System Design (Configuration) Guide* and check whether the amount of memory required to run JP1/AJS3 is secured.

KNBB6451-E

A system error has occurred. (*maintenance-information*)

A system error occurred.

(S)

The system aborts the process.

(O)

If maintenance information includes information about a memory shortage, follow the instructions in KNBB6450-E. Also, if the execution results (standard output) of the command executed from the service linkage monitoring job contain multi-byte characters, check whether the language type and character encoding used by JP1/AJS3 match. If they do not match, adjust the command execution results (standard output) or JP1/AJS3 settings.

If this is not the case, collect the data by using the data collection tool and contact your system administrator.

KNBB6452-E

An unexpected error occurred. (*maintenance-information*)

An unexpected error occurred.

(S)

The system aborts the process.

(O)

Collect the data by using the data collection tool and contact your system administrator.



Appendixes

A. Files and Directories

This appendix lists the files and directories for the JP1/AJS3 for Cloud Service Applications.

A.1 In Windows

The following table lists the files and folders for the Windows version of JP1/AJS3 for Cloud Service Applications.

Supplementary note

For the tables listing log files and directories, see [9.2.8 List of log files and directories](#).

How to read the tables

The tables listing files and directories use the following abbreviations:

Abbreviation	Folder indicated by the abbreviation
<i>CSA_Path</i>	JP1/AJS3 for Cloud Service Applications installation folder ^{#1}
<i>Csa_Data_Path</i>	The value is different depending on the installation folder. If the installation folder is the default installation folder or is in a folder protected by the system: %ALLUSERSPROFILE% ^{#2} \Hitachi\JP1\JP1_DEFAULT\JP1AJS3CSA A folder protected by the system is the path to a folder in any of the following: <ul style="list-style-type: none">• <i>system-drive</i>\Windows• <i>system-drive</i>\Program Files If the installation folder is other than the above: <i>JP1/AJS3 for Cloud Service Applications installation folder</i>
<i>Mgr_Path</i>	JP1/AJS3 - Manager installation folder ^{#3}
<i>Mgr_Data_Path</i>	JP1/AJS3 - Manager data folder ^{#3}
<i>Agt_Path</i>	JP1/AJS3 - Agent installation folder ^{#4}
<i>Agt_Data_Path</i>	JP1/AJS3 - Agent data folder ^{#4}
<i>View_Path</i>	JP1/AJS3 - View installation folder ^{#5}
<i>View_Data_Path</i>	JP1/AJS3 - View data folder ^{#5}

#1

By default, *CSA_Path* is *system-drive*\Program Files\HITACHI\JP1AJS3CSA.

#2

The default value for %ALLUSERSPROFILE% is *system-drive*\ProgramData.

#3

For details, see the description of *JP1/AJS3 - Manager files and directories* in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

#4

For details, see the description of *JP1/AJS3 - Agent files and directories* in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

#5

For details, see the description of *JP1/AJS3 - View files and directories* in the manual *JP1/Automatic Job Management System 3 Troubleshooting*.

Table A–1: List of the files and folders (In Windows)

Item	File or folder name	
	Normal configuration	Cluster configuration
Product folder	<i>Csa_Path</i> \	--
Executable file storage folder	<i>Csa_Path</i> \bin	--
Environment-settings file	<i>Csa_Path</i> \conf\ajs3csaweb.conf	<i>Shared-folder</i> \jplajs3csa\conf\ajs3csaweb.conf
Environment-settings model file	<i>Csa_Path</i> \conf\ajs3csaweb.conf.model	--
System files folder for Web interface	<i>Csa_Path</i> \sys\	<i>Shared-folder</i> \jplajs3csa\sys\
Configuration definition file	<i>Csa_Path</i> \sys\ajscsasetup.conf	--
Execution log of the JP1/AJS3 Web Application Server service	<i>Csa_Path</i> \sys\service.log	--
User information storage folder	<i>Csa_Path</i> \sys\user\	<i>Shared-folder</i> \jplajs3csa\sys\user\
Tool files storage folder	<i>Csa_Path</i> \tools\	--
Option definition file for J2EE server	<i>Csa_Path</i> \uCP SB\CC\server\usrconf\ejb\ajs3csa\usrconf.cfg	--
User property file for J2EE server	<i>Csa_Path</i> \uCP SB\CC\server\usrconf\ejb\ajs3csa\usrconf.properties	--
System property file for server management commands	<i>Csa_Path</i> \uCP SB\CC\admin\usrconf\usrconf.properties	--
Web server definition file	<i>Csa_Path</i> \uCP SB\httpsd\conf\httpsd.conf	--
Server private key	<i>Csa_Path</i> \uCP SB\httpsd\conf\ssl\server\httpsdkey.pem	--
SSL server certificate	<i>Csa_Path</i> \uCP SB\httpsd\conf\ssl\server\httpsd.pem	--
Application directory	<i>Csa_Path</i> \webapps\ajs3csa\	--
Product folder	<i>Csa_Data_Path</i> \	<i>Shared-folder</i> \jplajs3csa\
Environment-settings file storage folder	<i>Csa_Data_Path</i> \conf\	<i>Shared-folder</i> \jplajs3csa\conf\
Root certificate storage folder	<i>Csa_Data_Path</i> \conf\ssl\rootcer\	<i>Shared-folder</i> \jplajs3csa\conf\ssl\rootcer
Database storage folder	<i>Csa_Data_Path</i> \database\	<i>Shared-folder</i> \jplajs3csa\database
Communication configuration file for JP1/AJS3 - Agent (sample file)	<i>Agt_Data_Path</i> \conf\ajscsajob_network.conf.model	<i>Shared-folder</i> \jplajs2\conf\ajscsajob_network.conf.model
Communication configuration file for JP1/AJS3 - Manager (sample file)	<i>Mgr_Data_Path</i> \conf\ajscsajob_network.conf.model	<i>Shared-folder</i> \jplajs2\conf\ajscsajob_network.conf.model

Item	File or folder name	
	Normal configuration	Cluster configuration
Service linkage job or service linkage monitoring job operation command (registration)	<i>View_Path</i> \bin\ajscsajobreg.exe	--
Service linkage job or service linkage monitoring job operation command (listing)	<i>View_Path</i> \bin\ajscsajoblist.exe	--
Service linkage job or service linkage monitoring job operation command (deletion)	<i>View_Path</i> \bin\ajscsajobdel.exe	--
Service linkage definition information file storage folder	<i>View_Data_Path</i> \csadef	--
Service linkage monitoring definition information file storage folder	<i>View_Data_Path</i> \csadef\customevent	--
Service linkage objects monitoring job temporary file folder	<i>Agt_Data_Path</i> \sys\infoagt\ajscsaobjwatch#	<i>Shared-folder</i> \jplajs2\sys\infoagt\ajscsaobjwatch#

Legend:

--: Not applicable.

#

The *Agt_Data_Path* and *Shared-folder*\jplajs2 can be changed with the `WaitInFileOutDir` (for agent processes) environment setting parameter. For details, see *Details of the environment setting parameters for event/action control* in the manual *JP1/Automatic Job Management System 3 Configuration Guide*.

A.2 In Linux

The following table lists the files and folders for the Linux version of JP1/AJS3 for Cloud Service Applications.

Table A–2: List of the files and folders (In Linux)

Item	File or folder name	
	Normal configuration	Cluster configuration
Product directory	/opt/jplajs3csa/	--
Executable file storage directory	/opt/jplajs3csa/bin/	--
Environment-settings file	/etc/opt/jplajs3csa/conf/ajs3csaweb.conf	<i>Shared-directory</i> /jplajs3csa/conf/ajs3csaweb.conf
Environment-settings model file	/etc/opt/jplajs3csa/conf/ajs3csaweb.conf.model	--
System files directory for Web interface	/var/opt/jplajs3csa/sys/	<i>Shared-directory</i> /jplajs3csa/sys/
Configuration definition file	/var/opt/jplajs3csa/sys/ajscsasetup.conf	--
User information storage directory	/var/opt/jplajs3csa/sys/user/	<i>Shared-directory</i> /jplajs3csa/sys/user/
Tool files storage directory	/opt/jplajs3csa/tools/	--

Item	File or folder name	
	Normal configuration	Cluster configuration
Option definition file for J2EE server	/opt/jplajs3csa/uCPSB/CC/server/usrconf/ejb/ajs3csa/usrconf.cfg	--
User property file for J2EE server	/opt/jplajs3csa/uCPSB/CC/server/usrconf/ejb/ajs3csa/usrconf.properties	--
System property file for server management commands	/opt/jplajs3csa/uCPSB/CC/admin/usrconf/usrconf.properties	--
Web server definition file	/opt/jplajs3csa/uCPSB/httpsd/conf/httpsd.conf	--
Server private key	/opt/jplajs3csa/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem	--
SSL server certificate	/opt/jplajs3csa/uCPSB/httpsd/conf/ssl/server/httpsd.pem	--
Application directory	/opt/jplajs3csa/webapps/ajs3csa/	--
Product directory	/etc/opt/jplajs3csa/	--
Environment-settings file storage directory	/etc/opt/jplajs3csa/conf/	<i>Shared-directory</i> /jplajs3csa/conf/
Root certificate storage directory	/etc/opt/jplajs3csa/conf/ssl/rootcer/	<i>Shared-directory</i> /jplajs3csa/conf/ssl/rootcer
Database storage directory	/var/opt/jplajs3csa/database	<i>Shared-directory</i> /jplajs3csa/database/
Communication configuration file for JP1/AJS3 - Agent (sample file)	/etc/opt/jplajs2/conf/ajscsajob_network.conf.model	<i>Shared-directory</i> /jplajs2/conf/ajscsajob_network.conf.model
Communication configuration file for JP1/AJS3 - Manager (sample file)	/etc/opt/jplajs2/conf/ajscsajob_network.conf.model	<i>Shared-directory</i> /jplajs2/conf/ajscsajob_network.conf.model
Service linkage objects monitoring job temporary file directory	/var/opt/jplajs2/sys/infoagt/ajscsaobjwatch#	<i>Shared-directory</i> /jplajs2/sys/infoagt/ajscsaobjwatch#

Legend:

--: Not applicable.

#

/var/opt/jplajs2 and *Shared-directory*/jplajs2 can be changed with the WaitInFileOutDir (for agent processes) environment setting parameter. For details, see *Details of the environment setting parameters for event/action control* in the manual *JP1/Automatic Job Management System 3 Configuration Guide*.

B. Limitations

For details about limits on JP1/AJS3 for Cloud Service Applications, see the *Release Notes*.

C. Estimation

For details about the resources required for operations on JP1/AJS3 for Cloud Service Applications (the required memory size and disk utilization), see the *Release Notes*.

D. Port number to be set

This section explains the port number to be set and the direction through the firewall.

You can change the port number according to the user environment.

The protocol used is TCP/IP.

The following table shows the protocol number used in JP1/AJS3 for Cloud Service Applications.

Table D–1: Port number used in JP1/AJS3 for Cloud Service Applications

Purpose	Port number	Direction
Communication for transmitting or receiving HTTP requests or HTTP responses that occur as a result of operations on a Web browser ^{#1}	Non-SSL communication: 22265 SSL communication: 22266	Web browsers → JP1/AJS3 CSA HTTP Server service
Communication that occurs inside the JP1/AJS3 for Cloud Service Applications server and that occurs with an application server ^{#2}	22267	JP1/AJS3 CSA HTTP Server service → JP1/AJS3 CSA Web Application Server service
Communication ports for internal JP1/AJS3 for Cloud Service Applications server	22268	None.
Port for communication from a server management command to an application server ^{#2}	22269	Server management command → JP1/AJS3 CSA Web Application Server service
Communication for authenticating login requests ^{#1}	20240	JP1/Base → JP1/Base
Communication for transmitting or receiving HTTP requests or HTTP responses that occur as a result of execution of service linkage jobs or service linkage monitoring jobs ^{#1}	Non-SSL communication: 22265 SSL communication: 22266	Service linkage jobs or service linkage monitoring jobs → JP1/AJS3 CSA HTTP Server service

#1: When setting the firewall, specify the "Source port number" as "ANY".

#2: Communication within the same machine.

E. JP1/AJS3 Environment Setting Parameters

This section provides information about a list of environment setting parameters configured on JP1/AJS3 installed on the host that runs service linkage jobs or service linkage monitoring jobs of JP1/AJS3 for Cloud Service Applications. This section also provides information about definition of the environment setting parameters. For details on other environment setting parameters of the JP1/AJS3, see the description of *Environment Setting Parameters* in the manual *JP1/Automatic Job Management System 3 Configuration Guide*.

E.1 Format of the environment setting parameters

This section describes the format of the definition keys and environment setting parameters used in this manual.

(1) Format of the definition keys

Definition keys are written in the following format:

```
[name-of-definition-key]
```

- The name of each definition key name is enclosed in square brackets ([]).
- In the { JP1_DEFAULT | *logical-host-name* } part, enter JP1_DEFAULT for the physical host, and enter the name of a logical host for *logical-host-name*.

(2) Format of the environment setting parameters

Environment setting parameters are written in the following format:

```
"name-of-environment-setting-parameter"=definition
```

- The name of an environment setting parameter is enclosed in double quotation marks (").
- If a string is specified for a definition, the definition is enclosed in double quotation marks. If a numeric value is specified for a definition, `dword:` precedes the value.
- If multiple values are allowed for the definition of an environment setting parameter, the values are separated by a colon (:). Note that you must specify at least one value.

Example:

If the definition key is {backup:export:name:print:schedule:show:rgexport:release}, you can specify more than one of the following values:

backup, export, name, print, schedule, show, rgexport, and release

E.2 List of Environment Setting Parameters

The following table shows environment setting parameters of the JP1/AJS3 for Cloud Service Applications.

Table E-1: Environment setting parameters of the JP1/AJS3 for Cloud Service Applications

No	Definition key	Environment setting parameter	Definition	Applicable OS	Applicable product
1	[{JP1_DEFAULT <i>logical-host-name</i> } \JP1AJS2\CSA\CSAJ OBAGENT\AJSCSAEXE C]#	CSACONNECTCO NFIG	Specify the file name of the connection configuration file with JP1/AJS3 for Cloud Service Applications server	Windows Linux	M, A
2		JOBLOGSIZE	Specify the size of the service linkage job log file	Windows Linux	M, A
3		LimitObjMonS tdOutSize	Specify the maximum size of the standard output of commands run with monitoring processing for the service linkage objects monitoring job.	Windows Linux	M, A
4		CloudObjectM on	Set when using a service linkage objects monitoring job.	Windows Linux	M, A
5		LogSize_ajsc saobjmond	Specify the size of the service linkage objects monitoring log file.	Windows Linux	M, A
6		LogNumFiles_ ajscsaobjmon d	Specify the number of service linkage objects monitoring log files.	Windows Linux	M, A
7		OBJWLOGSIZE	Specify the size of the service linkage objects monitoring job log file.	Windows Linux	M, A
8		UACAdministr atorsExec	Setting to run monitoring processes of the service linkage objects monitoring job in the agent as an administrator with the UAC function enabled (Windows only)	Windows	M, A
9		LogonUserRet ryCount	Number of retries for acquiring an access token when running monitoring processes of the service linkage objects monitoring job in the agent (Windows only)	Windows	M, A
10		LogonUserRet ryInterval	Interval between retries for acquiring an access token when running monitoring processes of the service linkage objects monitoring job in the agent (Windows only)	Windows	M, A

Legend:

M: JP1/AJS3 - Manager

A: JP1/AJS3 - Agent

#:

Specify JP1_DEFAULT for the physical host. For *logical-host-name*, specify the name of a logical host.

Parameters that are not described here are used for maintenance purposes. Do not change the values of those parameters.

E.3 Details of the environment setting parameters

This subsection describes details of the environment setting parameters of the JP1/AJS3 for Cloud Service Applications.

Note that the default of an environment setting parameter means the value that is assumed when the environment setting parameter is omitted.

(1) CSACONNECTCONFIG

Specify the file name of the connection configuration file containing connection information with JP1/AJS3 for Cloud Service Applications server.

Format

"CSACONNECTCONFIG"="*file-name-of-the-connection-configuration-file-with-JP1/AJS3 for Cloud Service Applications server*"

Specifiable values

A character string of no more than 255 bytes

Default value

In Windows

- Physical host:
JP1/AJS3 installation-folder\conf\ajscsajob_network.conf
- Logical host:
shared-folder\jplajs2\conf\ajscsajob_network.conf

In Linux

- Physical host:
/etc/opt/jplajs2/conf/ajscsajob_network.conf
- Logical host:
shared-directory/jplajs2/conf/ajscsajob_network.conf

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

For service linkage jobs:

The next time running a service linkage job

For service linkage monitoring jobs:

The next time starting the JP1/AJS3 service

The next time running a service linkage job

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host does not take over to the logical host. After cluster setup, review the setting of this parameter.

(2) JOBLOGSIZE

Specify the size of the service linkage job log file.

Format

"JOBLOGSIZE"=dword:*size-of-the-service-linkage-job-log-file*

Specifiable values

A hexadecimal value (in KB) from 00006400 to 0001B800 (25,600 to 112,640 in decimal)

Default value

dword:00006400 (25,600 in decimal)

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

The next time running a service linkage job

Cautionary note

During cluster setup (jajs_setup_cluster execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(3) LimitObjMonStdOutSize

Specify the maximum size of the standard output of commands[#] run with monitoring processing for the service linkage objects monitoring job.

[#]: *Commands* refer to a command specified in the *command line* of the objects monitoring definition.

Format

"LimitObjMonStdOutSize"=dword:*maximum-size-of-the-standard-output-of-commands-run-with-monitoring-processing-for-the-service-linkage-objects-monitoring-job*

Specifiable values

A hexadecimal value (in KB) from 00000600 to 00001400 (1,536 to 5,120 in decimal)

Default value

dword:00000C00 (3,072 in decimal)

Recommended value

Default value

When the setting takes effect

When starting the JP1/AJS3 service

Cautionary note

During cluster setup (jajs_setup_cluster execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(4) CloudObjectMon

Set when using a service linkage objects monitoring job.

Format

"CloudObjectMon"={Y|N}

Specifiable values

Y

Start the service linkage objects monitoring job daemon.

N

Do not start the service linkage objects monitoring job daemon.

Default value

N

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

When starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(5) LogSize_ajscsaobjmond

Specify the size of the service linkage objects monitoring log file.

Format

"LogSize_ajscsaobjmond"=`dword`:*size-of-the-service-linkage-objects-monitoring-log-file*

Specifiable values

A hexadecimal value (in Byte) from 00020000 to 40000000 (131,072 to 1,073,741,824 in decimal)

Default value

`dword:00200000` (2,097,152 in decimal)

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

When starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(6) LogNumFiles_ajscsaobjmond

Specify the number of service linkage objects monitoring log files.

Format

"LogNumFiles_ajscsaobjmond"=`dword`:*number-of-service-linkage-objects-monitoring-log-files*

Specifiable values

A hexadecimal value from 00000002 to 00000010 (2 to 16 in decimal) (unit: number of files)

Default value

`dword:0000000D` (13 in decimal)

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

When next starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(7) OBJWLOGSIZE

Specify the size of the service linkage objects monitoring job log file.

Format

"OBJWLOGSIZE"=`dword: size-of-the-service-linkage-objects-monitoring-job-log-file`

Specifiable values

A hexadecimal value (in KB) from 00006400 to 0001B800 (25,600 to 112,640 in decimal)

Default value

`dword:00006400` (25,600 in decimal)

Recommended value

Set the value appropriate for the operating environment.

When the setting takes effect

When next starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(8) UACAdministratorsExec (Windows only)

Specify whether to run monitoring processes of the service linkage objects monitoring job in the agent as an administrator with the UAC function enabled.

Format

"UACAdministratorsExec"=`dword: whether-torun-as-administrator-with-UAC-function-enabled`

Specifiable values

0
When the UAC function is enabled, jobs executed by the OS user in the Administrators group are run with Administrator permissions disabled. However, this does not apply to the built-in Administrator or OS users in the same Administrators group as the JP1/AJS3 service accounts.

1
When the UAC function is enabled, jobs executed by the OS user in the Administrators group are run with Administrator permissions.

If 1 is specified, all OS users executing jobs (including standard users) must have *Log on as a batch job* rights.

Default value

`dword:00000000` (0 in decimal)

Recommended value

Default value

When the setting takes effect

When next starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(9) LogonUserRetryCount (Windows only)

Specify the number of retries for acquiring an access token when running monitoring processes of the service linkage objects monitoring job in the agent.

Format

"LogonUserRetryCount"=dword:*number-of-retries-to-acquire-an-access-token-when-running-a-monitoring-process-of-a-service-linkage-objects-monitoring-job-in-the-agent*

Specifiable values

A hexadecimal value from 00000000 to 00000064 (0 to 100 in decimal)

Specify a hexadecimal value of 00000000 (0 in decimal) to prevent retry attempts.

Default value

dword:00000003 (3 in decimal)

Recommended value

Default value

When the setting takes effect

When next starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

(10) LogonUserRetryInterval (Windows only)

Specify the interval between retries for acquiring an access token when running monitoring processes of the service linkage objects monitoring job in the agent.

Format

"LogonUserRetryInterval"=dword:*retry-interval-for-acquiring-an-access-token-when-running-a-monitoring-process-of-a-service-linkage-objects-monitoring-job-in-the-agent*

Specifiable values

A hexadecimal value from 00000001 to 0000012C (1 to 300 in decimal) (unit: seconds)

Default value

dword:00000001 (1 in decimal)

Recommended value

Default value

When the setting takes effect

When next starting the JP1/AJS3 service

Cautionary note

During cluster setup (`jajs_setup_cluster` execution) in JP1/AJS3, the value of the physical host takes over to the logical host

F. Service linkage job information definition files

This section explains the files that define the service linkage job information of JP1/AJS3 for Cloud Service Applications.

The service linkage job information definition files come in the following three types:

- Connection definition file (`slcondefExport.txt`)
- Execution definition file (`sldefExport.txt`)
- Service linkage job definition file (`sljobdefExport.txt`)

F.1 Connection definition file

The connection definition file can be downloaded by clicking **Export** on the Connection definitions screen or the Home screen where a connection definition was selected. If a connection definition file is specified by clicking **Import** on the Connection definitions screen and the connection definition file is specified, service linkage connection information can be imported to JP1/AJS3 for Cloud Service Applications.

The details of the connection definition file are as follows:

(1) Default connection definition file name

When **Export** is clicked on the Connection definitions screen

`slcondefExport.txt`

When **Export** is clicked on the Home screen where a connection definition was selected

`entered_slcondefExport.txt`

(2) Format of connection definition file

(a) For 13-00

```
{
  "name": "Definition name of connection definition information"
  "comment": "Description",
  "jplresource": "JPI resource group name",
  "productVersion": "Version information",
  "definitionKind": "CONNECTINFO",
  "callKind": "Call type of cloud service",
  "schemaVersion": "Schema version",
  "start": {
    "cli": {
      "commandLine": "Command line to be executed during connection start processing",
      "envValue": [
        {
          "name": "Environment variable name",
          "value": "Value of environment variable"
        }, ...
      ]
    },
    "resultVariable": "Variable name at setting destination of passing i
```

```

nformation",
  "abendInfo": {
    "condition": "Relational operator of abnormal end judgment condition",
    "value": Value of abnormal end judgment condition,
    "returnValue": Return value of job in case of abnormal end
  },
  "traceInfo": {
    "logFileOut": {
      "cliCommandLine": Whether trace information needs to be output to the CLI command line,
      "cliStdOut": Whether trace information needs to be output to the CLI command standard output,
      "cliStdErr": Whether trace information needs to be output to the CLI command standard error
    },
    "stderrOut": {
      "cliCommandLine": Whether trace information needs to be output to the CLI command line,
      "cliStdOut": Whether trace information needs to be output to the CLI command standard output,
      "cliStdErr": Whether trace information needs to be output to the CLI command standard error
    }
  }
},
"end": {
  "cli": {
    "commandLine": "Command line to be executed",
    "envValue": [
      {
        "name": "Environment variable name",
        "value": "Value of environment variable"
      },...
    ]
  },
  "abendInfo": {
    "condition": "Relational operator for abnormal end judgment condition",
    "value": Value of abnormal end judgment condition,
    "returnValue": Return value of job in case of abnormal end
  },
  "traceInfo": {
    "logFileOut": {
      "cliCommandLine": "Whether the CLI command line needs to be output",
      "cliStdOut": "Whether trace information needs to be output to the CLI command standard output",
      "cliStdErr": "Whether trace information needs to be output to the CLI command standard error output"
    },
    "stderrOut": {
      "cliCommandLine": "Whether trace information needs to be output to the CLI command line",
      "cliStdOut": "Whether trace information needs to be output to the CLI command standard output",
      "cliStdErr": "Whether trace information needs to be output to the CLI command standard error output"
    }
  }
}

```

```

    }
  },
  "parameters": [
    {
      "name": "Variable name",
      "type": "exec",
      "exec": {
        "type": "env",
        "value": "Value of variable"
      }
    },
    ...
  ],
  "overallEnvValue": [
    {
      "name": "Environment variable name",
      "value": "Value of environment variable"
    },
    ...
  ]
}

```

(b) For 13-10 or later

```

{
  "name": "Definition name of connection definition information",
  "comment": "Description",
  "jplresource": "JPI resource group name",
  "productVersion": "Version information",
  "definitionKind": "CONNECTINFO",
  "callKind": "Call type of cloud service",
  "schemaVersion": "Schema version",
  "start": {
    "cli": {
      "commandLine": "Command line to be executed during connection start processing",
      "envValue": [
        {
          "name": "Environment variable name",
          "value": "Value of environment variable"
        },
        ...
      ]
    },
    "resultVariable": "Variable name at setting destination of passing information",
    "abendInfo": {
      "condition": "Relational operator of abnormal end judgment condition",
      "value": "Value of abnormal end judgment condition",
      "returnValue": "Return value of job in case of abnormal end",
    },
    "abendInfoMon": {
      "detail": {
        "condition": "Relational operator for abnormal end judgment condition",
        "value": "Value of abnormal end judgment condition",
        "returnValue": "Return value of job in case of abnormal end",
        "abendExecResultOutput": {

```

```

        "cliCommandLine": "Whether trace information needs to be
output to the CLI command line,
        "cliStdOut": "Whether trace information needs to be output
to the CLI command standard output,
        "cliStdErr": "Whether trace information needs to be output
to the CLI command standard error"
    }
}
},
"traceInfo": {
    "logFileOut": {
        "cliCommandLine": "Whether the CLI command line needs to be
output",
        "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
        "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
    },
    "stderrOut": {
        "cliCommandLine": "Whether the CLI command line needs to be
output",
        "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
        "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
    }
},
"traceInfoMon": {
    "logFileOut": {
        "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
        "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
        "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
    },
}
},
"end": {
    "cli": {
        "commandLine": "Command line to be executed",
        "envValue": [
            {
                "name": "Environment variable name",
                "value": "Value of environment variable"
            },...
        ]
    },
    "abendInfo": {
        "condition": "Relational operator for abnormal end judgment cond
ition",
        "value": "Value of abnormal end judgment condition",
        "returnValue": "Return value of job in case of abnormal end"
    },
    "abendInfoMon": {
        "detail": {
            "condition": "Relational operator for abnormal end judgment
condition",

```

```

        "value": Value of abnormal end judgment condition,
        "returnValue": Return value of job in case of abnormal end
        "abendExecResultOutput": {
            "cliCommandLine": Whether trace information needs to be
output to the CLI command line,
            "cliStdOut": Whether trace information needs to be output
to the CLI command standard output,
            "cliStdErr": Whether trace information needs to be output
to the CLI command standard error
        }
    },
    "traceInfo": {
        "logFileOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
he CLI command standard error"
        },
        "stderrOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
he CLI command standard error"
        }
    },
    "traceInfoMon": {
        "logFileOut": {
            "cliCommandLine": Whether trace information needs to be outp
ut to the CLI command line,
            "cliStdOut": Whether trace information needs to be output t
o the CLI command standard output,
            "cliStdErr": Whether trace information needs to be output th
e CLI command standard error
        },
    }
},
"parameters": [
    {
        "name": "Variable name",
        "type": "exec",
        "exec": {
            "type": "env",
            "value": "Value of variable"
        }
    },
    ...
],
"overallEnvValue": [
    {
        "name": "Environment variable name",
        "value": "Value of environment variable"
    },
    ...
]

```

```

]
}

```

Legend:

. . . : Repetition of items enclosed "{" and "}" immediately before

(3) Items of connection definition file

The details of each item of the connection definition file are shown in the table below.

Table F-1: Items of connection definition file

Item				Description	
name				Definition name of connection definition information	
comment				Description of connection definition information	
jplresource				JP1 resource group of connection definition information	
productVersion				Version information of JP1/AJS3 for Cloud Service Applications	
definitionKind				Fixed to "CONNECTINFO"	
callKind				Call type of cloud service	
schemaVersion				Schema version of connection definition	
start	cli	commandLine		Command line to be executed during connection start processing	
		envValue	name	Environment variable name during connection start processing	
			value	Value of environment variable name during connection start processing	
	resultVariable			Variable name at setting destination of passing information during connection start processing	
	abendInfo	condition		Relational operator of abnormal end judgment condition during connection start processing	
		value		Value of abnormal end judgment condition during connection start processing	
		returnValue		Return value of job in case of abnormal end during connection start processing	
	abendInfoMon	detail	condition		Relational operator of abnormal end judgment condition during connection start processing of the monitoring job
			value		Value of abnormal end judgment condition during connection start processing of the monitoring job
			returnValue		Return value of job in case of abnormal end during connection start processing of the monitoring job
		abendExecResultOutput	cliCommandLine	Whether the CLI command line needs to be output in case of abnormal end during connection start processing of the monitoring job	
			cliStdOutput	Whether the CLI command standard output needs to be output during connection start processing of the monitoring job	
cliStdError			Whether the CLI command standard error output needs to be output in case of abnormal end during connection start processing of the monitoring job		

Item				Description	
start	traceInfo	logFileOutput	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the log file during connection start processing	
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the log file during connection start processing	
			cliStdErr	Whether trace information needs to be output to the CLI command standard error when it is to be output to the log file during connection start processing	
		stderrOutput	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the standard error output during connection start processing	
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the standard error output during connection start processing	
			cliStdErr	Whether trace information needs to be output the CLI command standard error output during connection start processing	
	traceInfoMon	logFileOutput	cliCommandLine	Whether the CLI command line needs to be output when trace information is output to the log file during connection start processing of the monitoring job	
			cliStdOut	Whether the CLI command standard output needs to be output when trace information is output to the log file during connection start processing of the monitoring job	
			cliStdErr	Whether the CLI command standard error output needs to be output when trace information is output to the log file during connection start processing of the monitoring job	
end	cli	commandLine		Command line to be executed during connection start processing	
		envValue	name	Environment variable name during connection termination processing	
			value	Value of environment variable during connection termination processing	
	abendInfo	condition		Relational operator for abnormal end judgment condition during connection termination processing	
		value		Value of abnormal end judgment condition during connection termination processing	
		returnValue		Return value of job in case of abnormal end during connection termination processing	
	abendInfoMon	detail	condition		Relational operator of abnormal end judgment condition during connection termination processing of the monitoring job
			value		Value of abnormal end judgment condition during connection termination processing of the monitoring job
			returnValue		Return value of job in case of abnormal end during connection termination processing of the monitoring job
		abendExecResultOutput	cliCommandLine	Whether the CLI command line needs to be output in case of abnormal end during connection termination processing of the monitoring job	

Item				Description
end	abendInfoMon	detail	abendExecResultOutput	Whether the CLI command standard output needs to be output during connection termination processing of the monitoring job
			cliStdErr	Whether the CLI command standard error output needs to be output in case of abnormal end during connection termination processing of the monitoring job
	traceInfo	logFileOutput	cliCommandLine	Whether the CLI command line needs to be output when trace information is to be output to the log file during connection termination processing
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is output to the log file during connection termination processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during connection termination processing
		stdErrOutput	cliCommandLine	Whether the CLI command line needs to be output when trace information is to be output to the log file during connection termination processing
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is output to the log file during connection termination processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during connection termination processing
	traceInfoMon	logFileOutput	cliCommandLine	Whether the CLI command line needs to be output when trace information is output to the log file during connection termination processing of the monitoring job
			cliStdOut	Whether the CLI command standard output needs to be output when trace information is output to the log file during connection termination processing of the monitoring job
cliStdErr			Whether the CLI command standard error output needs to be output when trace information is output to the log file during connection termination processing of the monitoring job	
parameters	name		Variable name for variable definition	
	type		Fixed to "exec"	
	exec	type	Fixed to "env"	
		value	Value of variable	
overallEnvValue	name		Environment variable name common to the whole	
	value		Value of environment variable common to the whole	

F.2 Execution definition file

The execution definition file can be downloaded by clicking **Export** on the Execution definition screen or the Home screen where an execution definition was selected. If the execution definition file is specified by clicking **Import** on the Execution definition screen, service linkage execution information can be imported to JP1/AJS3 for Cloud Service Applications.

The details of the execution definition file are as follows:

(1) Default execution definition file name

When **Export** is clicked on the Execution definitions screen

```
slexecdefExport.txt
```

When **Export** is clicked on the Home screen where an execution definition was selected

```
entered_slexecdefExport.txt
```

(2) Format of execution definition file

```
{
  "name": "Definition name of execution information",
  "comment": "Description",
  "jplresource": "JPI resource group name",
  "productVersion": "Version information",
  "definitionKind": "EXECINFO",
  "callKind": "Call type of cloud service",
  "schemaVersion": "Schema version",
  "exec": {
    "cli": {
      "commandLine": "Command line to be executed",
      "envValue": [
        {
          "name": "Environment variable name",
          "value": "Value of environment variable"
        }, ...
      ]
    },
    "resultVariable": "Setting destination variable name of passing information",
    "abendInfo": {
      "condition": "Relational operator for abnormal end judgment condition",
      "value": "Value of abnormal end judgment condition",
      "execAbendProc": "Whether abnormal end processing needs to be executing",
      "returnValue": "Return value of job in case of abnormal end"
    },
    "procCondition": {
      "comparisonSource": "Comparison source variable name",
      "normalEndCondition": [
        "Comparison destination of processing condition, ..."
      ],
      "abendSetting": {
        "execAbendProc": "Whether abnormal end processing needs to be executing",
        "returnValue": "Return value of job in case of abnormal end"
      }
    },
    "traceInfo": {
      "logFileOut": {
        "cliCommandLine": "Whether trace information needs to be output to CLI command line",
        "cliStdOut": "Whether trace information needs to be output t
```

```

o the CLI command standard output,
    "cliStdErr": Whether trace information needs to be output t
o the CLI command standard error output
    },
    "stderrOut": {
        "cliCommandLine": Whether trace information needs to be outp
ut to the CLI command line,
        "cliStdOut": Whether trace information needs to be output t
o the CLI command standard output,
        "cliStdErr": Whether trace information needs to be output t
o the CLI command standard error output
    }
},
"endJudgement": {
    "cli": {
        "commandLine": "Command line to be executing",
        "envValue": [
            {
                "name": "Environment variable name",
                "value": "Value of environment variable"
            },...
        ]
    },
    "resultVariable": "Setting destination variable name of passing info
rmation",
    "abendInfo": {
        "condition": "Relational operator of abnormal end judgment condi
tion",
        "value": Value of abnormal end judgment condition,
        "execAbendProc": "Whether abnormal end processing needs to be ex
ecuted in case of abnormal end",
        "returnValue": Return value of job in case of abnormal end
    },
    "procCondition": {
        "comparisonSource": "Comparison source variable name of processi
ng condition",
        "normalEndCondition": [
            Comparison destination of processing condition,...
        ],
        "continuing": {
            "continuingCondition": [
                Comparison destination of continuation condition,...
            ],
            "repeatInterval": Comparison destination of continuation con
dition,
            "numOfRepeat": Number of repetitions of continuation condi
tion,
            "execAbendProc": Whether execution of abnormal end processin
g needs to be executed,
            "returnValue": Return value of job when number of repetition
s of continuation condition is exceeded
        },
        "abendSetting": {
            "execAbendProc": "Whether abnormal end processing needs to b
e executed",
            "returnValue": Return value of job in case of abnormal end
        }
    }
}

```

```

    },
    "traceInfo": {
        "logFileOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
        },
        "stderrOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
        }
    }
},
"normalEndProc": {
    "cli": {
        "commandLine": "Command line to be executed",
        "envValue": [
            {
                "name": "Environment variable name",
                "value": "Value of environment variable"
            },...
        ]
    },
    "resultVariable": "Setting destination variable name of passing info
rmation",
    "abendInfo": {
        "condition": "Relational operator of abnormal end judgment condi
tion",
        "value": Value of abnormal end judgment condition,
        "returnValue": Return value of job in case of abnormal end
    },
    "traceInfo": {
        "logFileOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
        },
        "stderrOut": {
            "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
            "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
            "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
        }
    }
},
"abendProc": {

```

```

"cli": {
  "commandLine": "Command line to be executing",
  "envValue": [
    {
      "name": "Environment variable name",
      "value": "Value of environment variable"
    },...
  ]
},
"traceInfo": {
  "logFileOut": {
    "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
    "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
    "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
  },
  "stderrOut": {
    "cliCommandLine": "Whether trace information needs to be out
put to the CLI command line",
    "cliStdOut": "Whether trace information needs to be output t
o the CLI command standard output",
    "cliStdErr": "Whether trace information needs to be output t
o the CLI command standard error output"
  }
},
"outputResult": {
  "stdout": "Information to output the output of the execution result
as the standard output of a job",
  "stderrOut": "Information to output the output of the execution resu
lt as the standard error output of a job"
},
"parameters": [
  {
    "name": "Variable name of variable definition",
    "type": "Resolution type of variable",
    "gui": {
      "fieldName": "Label name",
      "controlType": "textBox"
      "textBoxSettings": {
        "lengthChar": String length,
        "invalidChar": "Characters prohibited from being input"
      }
    },
    "exec": {
      "type": "env",
      "value": "Value of variable"
    }
  },...
]
}

```

Legend:

. . . : Repetition of items enclosed "{" and "}" immediately before

(3) Items of execution definition file

The details of each item of the execution definition file are shown in the table below.

Table F-2: Items of execution definition file

Item				Description
name				Definition name of execution information
comment				Description of execution information
jplresource				JPI resource group name of execution information
productVersion				Version information of JP1/AJS3 for Cloud Service Applications
definitionKind				Fixed to "EXECINFO"
callKind				Call type of cloud service
schemaVersion				Schema version of execution definition
exec	cli	commandLine		Command line to be executed during execution processing
		envValue	name	Environment variable name during execution processing
			value	Value of environment variable during execution processing
	resultVariable			Setting destination variable name of passing information during execution processing
	abendInfo	condition		Relational operator for abnormal end judgment condition during execution processing
		value		Value of abnormal end judgment condition during execution processing
		returnValue		Return value of job in case of abnormal end during execution processing
	procCondition	comparisonSource		Comparison source variable name during execution processing
		normalEndCondition		Comparison destination of processing condition during execution processing
		abendSetting	execAbendProc	Whether abnormal end processing needs to be executing during abnormal end processing
			returnValue	Return value of job in case of abnormal end
	traceInfo	logFileOutput	cliCommandLine	Whether trace information needs to be output to CLI command line when it is to be output to the log file during execution processing
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is output to the log file during execution processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during execution processing
		stderrOutput	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the standard error output during execution processing
			cliStdOut	

Item				Description	
exec	traceInfo	stdErrOut	cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the standard error output during execution processing	
endJudgement	cli	commandLine		Command line to be executing during end judgment processing	
		envValue	name	Environment variable name during end judgment processing	
			value	Value of environment variable during end judgment processing	
	resultVariable			Setting destination variable name of passing information during end judgment processing	
	abendInfo	condition		Relational operator of abnormal end judgment condition during end judgment processing	
		value		Value of abnormal end judgment condition during end judgment processing	
		execAbendProc		Whether abnormal end processing needs to be executed in case of abnormal end during end judgment processing	
		returnValue		Return value of job in case of abnormal end during end judgment processing	
	procCondition	comparisonSource		Comparison source variable name of processing condition during end judgment processing	
		normalEndCondition			Comparison destination of processing condition during end judgment processing
		continuing	continuingCondition	Comparison destination of continuation condition during end judgment processing	
			repeatInterval	Repetition interval of continuation condition during end judgment processing	
			numOfRepeat	Number of repetitions of continuation condition during end judgment processing	
		abendSetting	execAbendProc	Whether execution of abnormal end processing needs to be executed during end judgment processing	
			returnValue	Return value of job when number of repetitions of continuation condition is exceeded during end judgment processing	
		traceInfo	logFileOutput	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the log file during end judgment processing
cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the log file during end judgment processing				
cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during end judgment processing				
stdErrOut	cliCommandLine		Whether trace information needs to be output to the CLI command line when it is to be output to the standard error output during end judgment processing		

Item				Description
endJudgement	traceInfo	stdErrOut	cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the standard error output during end judgment processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output standard error output during end judgment processing
normalEndProc	cli	commandLine		Command line to be executed during normal end processing
		envValue	name	Environment variable name during normal end processing
			value	Value of environment variable during normal end processing
	resultVariable			Setting destination variable name of passing information during normal end processing
	abendInfo	condition		Relational operator of abnormal end judgment condition during normal end processing
		value		Value of abnormal end judgment condition during normal end processing
		returnValue		Return value of job in case of abnormal end during normal end processing
	traceInfo	logFileOut	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the log file during normal end processing
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the log file during normal end processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during normal end processing
stdErrOut		cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the standard error output during normal end processing	
		cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the standard error output during normal end processing	
		cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the standard error output during normal end processing	
abendProc	cli	commandLine		Command line to be executing during abnormal end processing
		envValue	name	Environment variable name during abnormal end processing
			value	Value of environment variable during abnormal end processing
	traceInfo	logFileOut	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the log file during abnormal end processing
			cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the log file during abnormal end processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the log file during abnormal end processing
		stdErrOut	cliCommandLine	Whether trace information needs to be output to the CLI command line when it is to be output to the standard error output during abnormal end processing

Item				Description
abendProc	traceInfo	stdErrOut	cliStdOut	Whether trace information needs to be output to the CLI command standard output when it is to be output to the standard error output during abnormal end processing
			cliStdErr	Whether trace information needs to be output to the CLI command standard error output when it is to be output to the standard error output during abnormal end processing
outputResult	stdOut			Information to output the output of the execution result as the standard output of a job
	stdErrOut			Information to output the output of the execution result as the standard error output of a job
parameters	name			Variable name of variable definition
	type			Resolution type of variable. Either of the following values: <ul style="list-style-type: none"> "gui": Resolved on Detailed definition screen of JP1/AJS3 - View "exec": Resolved during execution of a job
	gui	fieldName		Label name of the input field in the case of resolution on the Detailed definition screen of JP1/AJS3 - View
		controlType		Fixed to "textBox"
		textBoxSettings	lengthChar	Character string length of the text box in the case of resolution on the Detailed definition screen of JP1/AJS3 - View
			invalidChar	Characters prohibited from being input to the text box in the case of resolution on the Detailed definition screen of JP1/AJS3 - View
	exec	type		Fixed to "exec"
		value		Value of variable in the case of resolution during job execution

F.3 Service linkage definition file

The service linkage job definition file can be downloaded by clicking **Export** on the Service linkage job definitions screen or the Home screen where a service linkage job definition was selected. When a service linkage job definition file is specified by clicking **Import** on the Service linkage job definition screen, service linkage job information can be imported to JP1/AJS3 for Cloud Service Applications.

The details of the service linkage job definition file are as follows:

(1) Default service linkage job definition file

When **Export** is clicked on the Service linkage job definition screen

`sljobdefExport.txt`

When **Export** is clicked on the Home screen where a service linkage job definition was selected

`entered_sljobdefExport.txt`

(2) Format of service linkage job definition file

```
{
    "name": "Definition name of service linkage job information",
    "comment": "Description",
```



```

    "jplresource": "JPI resource group name",
    "productVersion": "Version information",
    "definitionKind": "DEFINITIONINFO",
    "callKind": "Call type of cloud service",
    "schemaVersion": "Schema version",
    "slJobInfo": {
        "serviceName": "Linkage destination service name",
        "summary": "Overview of processing to be performed as linkage de
stination service",
        "execInfoName": "Definition name of execution information",
        "connectInfoName": "Definition name of connection information"
    }
}

```

(3) Items of service linkage job definition file

The details of each item of the service linkage definition file are shown in the table below.

Table F–3: Items of service linkage job definition file

Item	Description	
name	Definition name of service linkage job information	
comment	Description of service linkage job information	
jplresource	JPI group name of service linkage job information	
productVersion	Version information of JPI/AJS3 for Cloud Service Applications	
definitionKind	Fixed to "DEFINITIONINFO"	
callKind	Call type of cloud service	
schemaVersion	Schema version of service linkage job definition	
slJobInfo	serviceName	Linkage destination service name of service linkage job
	summary	Overview of processing to be performed as linkage destination service
	execInfoName	Definition name of execution information the format of " <i>/Execution-information-definition-name</i> "
	connectInfoName	Definition name of connection information in the format of " <i>/Connection-definition-name</i> "

G. Service linkage monitoring job information definition files

This section explains the files that define the service linkage monitoring job information of JP1/AJS3 for Cloud Service Applications.

The service linkage monitoring job information definition files come in the following three types:

- Connection definition file (`slcondefExport.txt`)
- Service linkage objects monitoring definition file (`slobjmondefExport.txt`)
- Service linkage monitoring job definition file (`slmonjobdefExport.txt`)

For details of connection definition files, see [F.1 Connection definition file](#). Only 13-10 and later format connection definition files can be used from the service linkage monitoring job.

G.1 Service linkage objects monitoring definition file

The service linkage objects monitoring definition file can be downloaded by clicking **Export** on the Object monitoring definition screen or the Home screen where an object monitoring definition is selected. If a service linkage objects monitoring definition file is specified by clicking **Import** on the Object monitoring definition screen, service linkage objects monitoring information can be imported to JP1/AJS3 for Cloud Service Applications.

The details of the service linkage objects monitoring definition file are as follows:

(1) Default service linkage objects monitoring definition file name

When **Export** is clicked on the Object monitoring definition screen

```
slobjmondefExport.txt
```

When **Export** is clicked on the Home screen where an object monitoring definition is selected

```
entered_slobjmondefExport.txt
```

(2) Format of service linkage objects monitoring definition file

```
{
  "name": "Definition name of service linkage objects monitoring information",
  "comment": "Description",
  "jplresource": "JPI resource group name",
  "productVersion": "Version information",
  "definitionKind": OBJECTMONITORINGINFO,
  "callKind": "Call type of cloud service",
  "schemaVersion": "Schema version",
  "ev": {
    "cli": {
      "commandLine": "Command line to be executed during connection start processing",
      "envValue": [
        {
          "name": "Environment variable name",
          "value": "Value of environment variable"
        }, ...
      ]
    }
  }
}
```

```

    },
    "monitoringInfo": {
      "objectInfo": {
        "name": "Variable name used for object name",
        "value": "Value specified for object name"
      },
      "updateInfo": [
        {
          "name": "Variable name used for update monitoring target item",
          "value": "Value specified as update monitoring target item"
        }, ...
      ]
    },
    "abendInfo": {
      "condition": "Relational operator of abnormal end judgment condition",
      "value": "Value of abnormal end judgment condition",
      "abendStopMonitoringInfo": {
        "returnValue": "Return value of job in case of abnormal end",
        "abendExecResultOutput": {
          "cliCommandLine": "Whether trace information needs to be output to the CLI command line",
          "cliStdOut": "Whether trace information needs to be output to the CLI command standard output",
          "cliStdErr": "Whether trace information needs to be output to the CLI command standard error"
        }
      },
      "logFileOut": {
        "cliStdOut": "Whether trace information needs to be output to the CLI command line"
      }
    },
    "traceInfo": {
      "logFileOut": {
        "cliCommandLine": "Whether trace information needs to be output to the CLI command line",
        "cliStdErr": "Whether trace information needs to be output to the CLI command standard error"
      }
    },
    "passingInfo": [
      {
        "name": "Passing information name",
        "value": "Value set in passing information"
      }, ...
    ],
    "parameters": [
      {
        "name": "Variable name",
        "type": "Variable resolution type",
        "gui": {
          "fieldName": "Label name",
          "controlType": "textBox"
          "textBoxSettings": {

```

```

        "lengthChar": String length,
        "invalidChar": "Characters prohibited from being input"
    }
},
"exec": {
    "type": "env",
    "value": "Value of variable"
}
},...
]
}

```

Legend:

. . . : Repetition of items enclosed "{" and "}" immediately before

(3) Items of service linkage objects monitoring definition file

The details of each item of the service linkage objects monitoring definition file are shown in the table below.

Table G–1: Items of service linkage objects monitoring definition file

Item			Description	
name			Definition name of service linkage objects monitoring definition information	
comment			Description of service linkage objects monitoring definition information	
jplresource			JP1 resource group of service linkage objects monitoring definition information	
productVersion			Version information of JP1/AJS3 for Cloud Service Applications	
definitionKind			Fixed to "OBJECTMONITORINGINFO"	
callKind			Call type of cloud service	
schemaVersion			Schema version of service linkage objects monitoring definition	
ev	cli	commandLine	Command line to be executed during service linkage objects monitoring processing	
		envValue	name	Environment variable name during service linkage objects monitoring processing
			value	Value of environment variable during service linkage objects monitoring processing
	monitoringInfo	objectInfo	name	Variable name used for object name. Fixed to ?CSAONAME?
			value	Value specified as object name
		updateInfo	name	Variable name for storing the specified value of the update monitoring target item. Fixed to ?CSAOINFO1? to ?CSAOINFO3?
			value	Value specified as update monitoring target item
	abendInfo	condition	Relational operator of abnormal end	

Item			Description		
ev	abendInfo	condition		judgment condition during service linkage objects monitoring processing	
		value		Value of abnormal end judgment condition during service linkage objects monitoring processing	
		abendStopMonitoringInfo	returnValue		Return value of job in case of abnormal end during service linkage objects monitoring processing
			abendExecResultOutput	cliCommandLine	Whether the CLI command line needs to be output in case of abnormal end during service linkage objects monitoring processing
				cliStdOut	Whether the CLI command standard output needs to be output in case of abnormal end during service linkage objects monitoring processing
				cliStdErr	Whether the CLI command standard error output needs to be output in case of abnormal end during service linkage objects monitoring processing
	logFileOutput	cliStdOut	Whether the CLI command standard output needs to be output to the log file in case of abnormal end during service linkage objects monitoring processing		
		traceInfo	logFileOutput	cliCommandLine	Whether the CLI command line needs to be output when trace information is output to the log file during service linkage objects monitoring processing
				cliStdErr	Whether the CLI command standard error needs to be output when trace information is output to the log file during service linkage objects monitoring processing
passingInfo	name		The passing information name of the service linkage objects monitoring job		
	value		Value set to passing information of the service linkage objects monitoring job		
parameters	name		Variable name of variable definition		
	type		Resolution type of variable. Either of the following values: <ul style="list-style-type: none"> "gui": Resolved on Detailed definition screen of JP1/AJS3 - View "exec": Resolved during execution of a job 		
	gui	fieldName		Label name of the input field in the case of resolution on the Detailed definition screen of JP1/AJS3 - View	
		controlType		Fixed to "textBox"	
		textBoxSettings	lengthChar		Character string length of the text box in the case of resolution on the Detailed definition screen of JP1/AJS3 - View
			invalidChar		Characters prohibited from being input to the text box in the case of resolution on the Detailed definition screen of JP1/AJS3 - View
	exec	type		Fixed to "env"	
		value		Value of variable in the case of resolution during job execution	

G.2 Service linkage monitoring job definition file

The service linkage monitoring job definition file can be downloaded by clicking **Export** on the Service linkage monitoring job definition screen or the Home screen where a service linkage monitoring job definition is selected. If the service linkage monitoring job definition file is specified by clicking **Import** on the Service linkage monitoring job definition screen, service linkage monitoring job information can be imported to JP1/AJS3 for Cloud Service Applications.

The details of the service linkage monitoring job definition file are as follows:

(1) Default service linkage monitoring job definition file name

When **Export** is clicked on the Service linkage monitoring job definition screen

```
slmonjobdefExport.txt
```

When **Export** is clicked on the Home screen where the service linkage monitoring job definition is selected

```
entered_slmonjobdefExport.txt
```

(2) Format of service linkage monitoring job definition file

```
{
  "name": "Definition name of service linkage monitoring job information"
  "comment": "Description",
  "jplresource": "JPI resource group name",
  "productVersion": "Version information",
  "definitionKind": DEFINITIONMONITORINGINFO,
  "callKind": "Call type of cloud service",
  "schemaVersion": "Schema version",
  "slMonitoringJobInfo": {
    "serviceName": "Linked service name",
    "summary": "Overview of linkage processing",
    "monitorInfoName": "Service linkage monitoring information definitio
n name",
    "connectInfoName": "Service linkage connection information definitio
n name"
  }
}
```

(3) Items of service linkage monitoring job definition file

The details of each item of the service linkage monitoring job definition file are shown in the table below.

Table G–2: Items of service linkage monitoring job definition file

Item	Description
name	Definition name of service linkage monitoring job information
comment	Description of service linkage monitoring job information
jplresource	JPI resource group name of service linkage monitoring job information
productVersion	Version information of JP1/AJS3 for Cloud Service Applications
definitionKind	Fixed to "DEFINITIONMONITORINGINFO"
callKind	Call type of cloud service

Item		Description
schemaVersion		Schema version of service linkage monitoring job definition
slMonitoringJobInfo	serviceName	Linked service name of service linkage monitoring job
	summary	Overview of processing to be performed as linkage destination service
	monitorInfoName	Definition name of monitoring information in the format of " <i>/Monitoring-information-definition-name</i> ".
	connectInfoName	Definition name of connection information in the format of " <i>/Connection-definition-name</i> ".

H. Version Revisions

H.1 Revisions in 13-10

- Service linkage monitoring jobs and service linkage objects monitoring jobs were added.
- Added following messages:
KNBB2418-W, KNBB2419-W, KNBB3035-I, KNBB4003-E, KNBB4011-E, KNBB6005-I, KNBB6011-I, KNBB6012-I, KNBB6013-I, KNBB6014-I, KNBB6015-I, KNBB6016-I, KNBB6017-I, KNBB6018-W, KNBB6102-E, KNBB6103-E, KNBB6104-W, KNBB6105-E, KNBB6106-E, KNBB6107-E, KNBB6150-E, KNBB6151-W, KNBB6152-E, KNBB6153-E, KNBB6154-E, KNBB6155-E, KNBB6156-E, KNBB6157-E, KNBB6158-E, KNBB6159-E, KNBB6160-E, KNBB6161-E, KNBB6162-W, KNBB6163-E, KNBB6164-E, KNBB6306-E, KNBB6307-W, KNBB6308-W, KNBB6309-E, KNBB6310-E, KNBB6311-E, KNBB6312-E, KNBB6402-E, KNBB6403-W, KNBB6449-E
- Changed following messages or description of messages:
KNBB2402-Q, KNBB2407-Q, KNBB2408-Q, KNBB2409-Q, KNBB2410-Q, KNBB2411-E, KNBB2412-I, KNBB2413-I, KNBB2415-E, KNBB2417-E, KNBB3291-E, KNBB4002-E, KNBB4003-E, KNBB4501-I, KNBB4508-E, KNBB4511-E, KNBB4512-E, KNBB4514-W, KNBB4515-I, KNBB4517-E, KNBB4518-E, KNBB4519-E, KNBB4520-E, KNBB4523-E, KNBB4524-E, KNBB4525-E, KNBB4526-W, KNBB6004-I, KNBB6200-E, KNBB6201-E, KNBB6203-E, KNBB6301-E, KNBB6450-E, KNBB6451-E
- Deleted following messages:
KNBB2559-E, KNBB2707-E, KNBB3201-E, KNBB3202-E, KNBB3203-E, KNBB3204-E, KNBB3206-E, KNBB3207-E

I. Reference Material for This Manual

I.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

About JP1/AJS3:

- *JP1 Version 13 Job Management: Getting Started (Job Scheduler)* (3021-3-L41(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Overview* (3021-3-L42(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 System Design (Configuration) Guide* (3021-3-L43(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3021-3-L44(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Configuration Guide* (3021-3-L45(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Administration Guide* (3021-3-L46(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Troubleshooting* (3021-3-L47(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Operator's Guide* (3021-3-L48(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Command Reference* (3021-3-L49(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Linkage Guide* (3021-3-L50(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 Messages* (3021-3-L51(E))
- *JP1 Version 13 JP1/Automatic Job Management System 3 for Enterprise Applications Description, User's Guide and Reference* (3021-3-L54(E))

About JP1:

- *JP1 Version 13 JP1/Base User's Guide* (3021-3-L09(E))
- *JP1 Version 13 JP1/Base Messages* (3021-3-L10(E))
- *JP1 Version 13 JP1/Base Function Reference* (3021-3-L11(E))

I.2 Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	<p>Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example:</p> <ul style="list-style-type: none">• From the File menu, choose Open• Click the Cancel button• In the Enter name entry box, type your name.
<i>Italic</i>	<p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none">• Write the command as follows: <code>copy source-file target-file</code>• The following message appears: A file was not found. (file = <i>file-name</i>) <p>Italic characters are also used for emphasis. For example:</p>

Text formatting	Convention
<i>Italic</i>	<ul style="list-style-type: none"> Do not delete the configuration file.
Monospace	<p>Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> At the prompt, enter <code>dir</code>. Use the <code>send</code> command to send mail. The following message is displayed: <code>The password is incorrect.</code>

The following table explains the symbols used in this manual:

Symbol	Convention
*	Multiplication sign
/	Division sign
↑ ↑	<p>The calculation result is rounded up to the next whole number.</p> <p>Example: The result of $\uparrow 34 / 3 \uparrow$ is 12.</p>
MAX	<p>Choose the largest of the calculation results.</p> <p>Example: The result of MAX (3 * 6, 4 + 7) is 18.</p>

I.3 Use of folder names and directory names

If a Windows folder name is the same as a UNIX directory name, they are treated as folder names in principle.

I.4 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation			Full name or meaning
JP1/AJS	JP1/AJS3	JP1/AJS3 - Manager	JP1/Automatic Job Management System 3 - Manager
		JP1/AJS3 - Agent	JP1/Automatic Job Management System 3 - Agent
		JP1/AJS3 - View	JP1/Automatic Job Management System 3 - View
	JP1/AJS2	JP1/AJS2 - Manager	JP1/Automatic Job Management System 2 - Manager
		JP1/AJS2 - Agent	JP1/Automatic Job Management System 2 - Agent
		JP1/AJS2 - View	JP1/Automatic Job Management System 2 - View
JP1/AJS3 - Web Console			JP1/Automatic Job Management System 3 - Web Console
JP1/AJS3 - Definition Assistant			JP1/Automatic Job Management System 3 - Definition Assistant
JP1/AJS3 for Enterprise Applications			JP1/Automatic Job Management System 3 for Enterprise Applications

Abbreviation		Full name or meaning	
JP1/AJS3 for Cloud Service Applications		JP1/Automatic Job Management System 3 for Cloud Service Applications	
JP1/AJS3 for CSA			
JP1/AJS3 CSA			
CSA			
Firefox	Firefox ESR	Mozilla(R) Firefox(R) Extended Support Release	
Linux	Linux 7	Red Hat Enterprise Linux(R) Server 7.1	
	Linux 8	Red Hat Enterprise Linux(R) Server 8	
	Linux 9	Red Hat Enterprise Linux(R) Server 9	
	Oracle Linux	Oracle Linux 7	Oracle Linux(R) Operating System 7
		Oracle Linux 8	Oracle Linux(R) Operating System 8
		Oracle Linux 9	Oracle Linux(R) Operating System 9
	SUSE Linux	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
SUSE Linux 15		SUSE Linux(R) Enterprise Server 15	

I.5 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
CLI	Command Line Interface
CN	Common Name
DNS	Domain Name System
GUI	Graphical User Interface
NAT	Network Address Translator
NAPT	Network Address Port Translation
OS	Operating System
PC	Personal Computer
PEM	Privacy Enhanced Mail
SAN	Subject Alternative Name
SSL	Secure Socket Layer
TLS	Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol

I.6 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

J. Glossary

This section explains the meaning of technical terms related to JP1/AJS3 for Cloud Service Applications. If you wish to read the JP1/AJS glossary, refer to the *Glossary* in the manual *JP1/Automatic Job Management System 3 Overview*.

A

Authentication definition

Definition of cloud service linkage authentication information.

C

Cloud computing

A computing model that provides computer resources as services by taking advantage of computer resources distributed over computer networks (such as the internet). This computing model can simply be referred to as a cloud.

Cloud service

A service that adopts cloud computing and is provided to users.

Cloud service linkage authentication information

Authentication information required for the interface to establish connection to a cloud service. This information can also be referred to as service linkage authentication information or authentication information.

Cloud service linkage connection information

Information about the interface for connecting to a cloud service. This information can also be referred to as service linkage connection information or connection information.

Cloud service linkage execution information

Information about the interface that enables the use of a cloud service after connection is established to the cloud service. This information can also be referred to as service linkage execution information or execution information.

Cloud service linkage information

A general term used to refer to cloud service linkage connection information, cloud service linkage authentication information, cloud service linkage execution information, and cloud service linkage monitoring information.

Cloud service linkage monitoring information

Information about the interface used for monitoring the cloud service status and other information after connection is established to the cloud service. This information can also be referred to as *service linkage monitoring information* or *monitoring information*.

Cloud service linkage objects monitoring information

Information about the interface used for monitoring cloud service objects in cloud service linkage monitoring information. This information can also be referred to as *service linkage objects monitoring information* or *objects monitoring information*.

Connection definition

Definition of cloud service linkage connection information.

E

Execution definitions

Definition of cloud service linkage execution information.

J

JP1/AJS

A generic name for JP1/Automatic Job Management System 3.

JP1/AJS is a program that automates work tasks.

In JP1/AJS, you can define sequences of tasks to execute at regular intervals, or have certain processing start when a specific event occurs.

JP1/AJS3

An abbreviation of JP1/Automatic Job Management System 3.

JP1/AJS3 - Agent

An abbreviation of JP1/Automatic Job Management System 3 - Agent.

JP1/AJS3 - Manager

An abbreviation of JP1/Automatic Job Management System 3 - Manager.

JP1/AJS3 - View

An abbreviation of JP1/Automatic Job Management System 3 - View.

JP1/AJS3 - Web Console

An abbreviation of JP1/Automatic Job Management System 3 - Web Console.

JP1/AJS3 for Cloud Service Applications

An abbreviation of JP1/Automatic Job Management System 3 for Cloud Service Applications.

JP1/Base

A program that provides the event service function. JP1/Base allows you to control the order in which services start, and it lets you send and receive JP1 events. JP1/Base is a prerequisite program for JP1/IM and JP1/AJS3. When JP1/IM is deployed in a system with JP1/AJS3, JP1/Base provides functionality for restricting operations by JP1 users.

L

Linkage job

A general term used to refer to service linkage jobs and service linkage monitoring jobs.

Linkage job information

A general term used to refer to service linkage job information and service linkage monitoring job information.

M

Monitoring definition

The cloud service linkage monitoring information definition.

Monitoring information

Cloud service linkage monitoring information.

O

Object monitoring definition

The cloud service linkage objects monitoring information definition.

Object monitoring information

Cloud service linkage objects monitoring information.

On-premises

A computing model in which software is installed and run on devices (for example, servers) installed in facilities or equipment managed by users.

On-premises environment

A computing environment that adopts the on-premises model.

S

Service linkage authentication information

This is the same as cloud service linkage authentication information.

Service linkage connection information

This is the same as cloud service linkage connection information.

Service linkage definition information file

A file that defines the following: (1) items that the user should enter in the Detailed Definition window of JP1/AJS3 - View, and (2) information required for execution of a service linkage job (for example, the host name of the JP1/AJS3 for Cloud Service Applications server).

You can output this file from JP1/AJS3 for Cloud Service Applications and import the file when registering a service linkage job in JP1/AJS3 - View.

The service linkage definition information file can also be referred to as a file for recording a custom job.

Service linkage execution information

This is the same as cloud service linkage execution information.

Service linkage information

Cloud service linkage information.

Service linkage job

A custom job that runs in tandem with a service provided by JP1/AJS3 for Cloud Service Applications. Service linkage jobs can be defined in JP1/AJS3 - View.

Service linkage job information

A series of information parts that are created from a set of information required for connecting to, authenticating, and executing a cloud service. Service linkage job information consists of the following three types of information: cloud service linkage connection information, cloud service linkage authentication information, and cloud service linkage execution information.

Service linkage monitoring definition information file

A file that defines the following: (1) items that the user should enter in the Detailed Definition window of JP1/AJS3 - View, and (2) information required for execution of a service linkage monitoring job (for example, the host name of the JP1/AJS3 for Cloud Service Applications server).

You can output this file from JP1/AJS3 for Cloud Service Applications and import the file when registering a service linkage monitoring job in JP1/AJS3 - View.

Service linkage monitoring information

Cloud service linkage monitoring information.

Service linkage monitoring job

A custom job that runs in tandem with a service provided by JP1/AJS3 for Cloud Service Applications to monitor the service. Service linkage monitoring jobs can be defined in JP1/AJS3 - View.

Service linkage monitoring job information

A series of information parts that are created from a set of information required for connecting to, authenticating, and executing a cloud service. Service linkage monitoring job information consists of the following three types of information: cloud service linkage connection information, cloud service linkage authentication information, and cloud service linkage monitoring information.

Service linkage objects monitoring information

Cloud service linkage objects monitoring information.

Service linkage objects monitoring job

A custom service linkage monitoring job used to monitor service objects that can be defined in JP1/AJS3 - View.

Web GUI

The Web GUI is the client terminal interface used to define information about service linkage jobs for JP1/AJS3 for Cloud Service Applications. You must establish a connection from a client terminal to the JP1/AJS3 for Cloud Service Applications server to display the Web GUI on your web browser.

Index

A

- [ajscsajobdel](#) 232
- [ajscsajoblist](#) 228
- [ajscsajobreg](#) 225
- [ajscsasetup](#) 205
- [Application Server Common Logs](#) 238
- [Application Server Logs](#) 239
- [Application server logs \(for executing service linkage monitoring jobs\)](#) 239
- [argument](#) 202
- [Authentication definitions window](#) 192
 - [Additional information item](#) 194
 - [ID/user](#) 193
 - [Security information/password](#) 193
- [authentication information](#) 19

B

- [Backing up](#) 89
- [Backing up and recovering the entire system](#) 91
- [Backup and recovery](#) 89
- [Behavior when the JP1/AJS3 service is started and stopped](#) 136

C

- [CAFile](#) 84
- [Changing the settings during operation](#) 54
- [cloud service linkage authentication information](#) 19
- [cloud service linkage connection information](#) 19
- [cloud service linkage execution information](#) 19
- [Cloud service linkage monitoring information](#) 20
- [Collecting data for troubleshooting](#) 254
- [Collecting data for troubleshooting in Linux](#) 256
- [Collecting data for troubleshooting in Windows](#) 254
- [COM_LOG_LANG](#) 64
- [COM_LOG_LEVEL](#) 63
- [COM_LOG_NUM](#) 64
- [COM_LOG_SIZE](#) 63
- [command](#)
 - [ajscsajobdel](#) 232
 - [ajscsajoblist](#) 228
 - [ajscsajobreg](#) 225
 - [ajscsasetup](#) 205
 - [jajs_csa](#) 209
 - [jajs_csa_stop](#) 211

- [jajs_log](#) 213
- [jajs_log.bat](#) 219
- [command description format](#) 202
- [Command Log](#) 240
- [commands](#)
 - [how to specify](#) 202
- [Commands](#) 201
- [Common display items](#) 146
- [Configuration file](#) 58
- [Configuration in cluster system](#) 34
- [Connection configuration file](#) 81
- [connection definition file](#)
 - [format](#) 361
 - [items](#) 366
- [Connection definition file](#) 361
- [Connection definitions window](#) 179
 - [Common environment variable settings](#) 181
 - [Connection termination processing](#) 187
 - [Setting variables dialog box](#) 191
 - [Variable settings](#) 182
- [Connection definition window](#)
 - [Connection processing](#) 183
- [connection information](#) 19
- [ConnectTimeout](#) 83
- [Considering the method for managing authentication information corresponding to the commands to be executed](#) 96
- [Consider system configuration](#) 24
- [CSAConnectPortNumber](#) 83
- [CSAConnectProtocol](#) 82
- [CSAConnectRetryCount](#) 84
- [CSAConnectRetryInterval](#) 84
- [CSAServerName](#) 82

D

- [data collection tool](#) 213, 219
- [Data to be collected when a problem occurs](#) 250
- [Data to collect](#) 250
- [Define Details window for service linkage jobs](#) 197
- [Definition flow of a linkage job](#) 101
- [Definition items of linkage job information](#) 102
- [Definition items of service linkage jobs](#) 109
- [Definition items of service linkage monitoring jobs](#) 110
- [Description format of unit definition parameters of service linkage jobs](#) 116

Description format of unit definition parameters of service linkage monitoring jobs 118

Designing and Building the System 37

Designs and definitions of linkage jobs 94

Designs of linkage jobs 95

Details of service linkage jobs 123

Details of service linkage objects monitoring jobs 130

Details of setting items of the environment setting file (ajs3csaweb.conf) 58

Details of the unit definition parameters of service linkage jobs 116

Details of the unit definition parameters of service linkage monitoring jobs 118

Details on the settings in the HTTP server definition file (httpspd.conf) 70

E

environment setting parameter

- CloudObjectMon 357
- CSACONNECTCONFIG 356
- JOBLOGSIZE 356
- LimitObjMonStdOutSize 357
- LogNumFiles_ajscsaobjmond 358
- LogonUserRetryCount 360
- LogonUserRetryInterval 360
- LogSize_ajscsaobjmond 358
- OBJWLOGSIZE 359
- UACAdministratorsExec 359

Environment variables for command execution 123

Escaping a command line for cloud service linkage information 104

Estimation 352

execution definition file 368

- format 369
- items 373

Execution definitions window 153

- Job output processing 170
- Linkage processing settings 157
- Setting variables dialog box 170
- Variable settings 155

execution information 19

Execution of service linkage jobs 122

Execution results of service linkage jobs 123

Execution results of service linkage objects monitoring jobs 139

F

Features of JP1/AJS3 for Cloud Service Applications 17

Files and Directories 347

Forced termination of service linkage objects monitoring jobs 139

Format of message explanations 264

H

HNTR_LOG_LANG 62

HNTR_LOG_LEVEL 61

Home window 146

how to collect data when a problem occurs 254

how to solve 258

I

Icon of service linkage jobs 112

Installation

- Linux 39
- windows 38

J

jajs_csa 209

jajs_csa_stop 211

jajs_log 213

jajs_log.bat 219

JP1/AJS3 Environment Setting Parameters 354

JP1/AJS3 for Cloud Service Applications database file 86

JP1/AJS3 - View Define Details window 197

K

Killing of service linkage jobs 124

L

Limitations 351

List of log files and directories 242

List of messages 275

- Messages beginning with KNBB 275

List of output destinations for messages 266

- Output destinations of messages beginning with KNBB 266

Login window 145

logs

- types and storage location 237

M

- Management operation of service linkage jobs 121
- Management operation of service linkage monitoring jobs 127
- Message format 264
- Message ID 264
- Messages 263
- Monitoring functions of service linkage objects monitoring jobs 130
- monitoring information 20
- Monitoring processing settings 175

N

- Notes on Define Details window 199
- Notes on execution of service linkage jobs 126
- Notes on execution of service linkage objects monitoring jobs 141
- Notes on linkage jobs 115
- Notes on Web GUI 195
- Notes when running anti-virus software 92

O

- Object monitoring definition window 172
- object monitoring information 20
- Operation in disaster-recovery configuration 36
- Operation of service linkage monitoring jobs 114
- option 202
- Option definition file for J2EE server 76

P

- Passing information of service linkage objects monitoring jobs 137
- Port number to be set 353
- Prerequisites of cluster system 34
- ProxyAddr 83

R

- Recovering 91
- Return codes of service linkage jobs 125
- Return codes of service linkage objects monitoring jobs 140

S

- SERVER_LOG_APP_LEVEL 65
- SERVER_LOG_APP_MON_LEVEL 67
- SERVER_LOG_APP_MON_NUM 67

- SERVER_LOG_APP_MON_SIZE 67
- SERVER_LOG_APP_NUM 65
- SERVER_LOG_APP_SIZE 64
- SERVER_LOG_JOB_LEVEL 66
- SERVER_LOG_JOB_MON_LEVEL 68
- SERVER_LOG_JOB_MON_NUM 68
- SERVER_LOG_JOB_MON_SIZE 67
- SERVER_LOG_JOB_NUM 66
- SERVER_LOG_JOB_SIZE 66
- SERVER_LOG_LANG 65
- SERVER_SESSION_TIMEOUT 69
- Server Job Logs 240
- service linkage authentication information 19
- service linkage connection information 19
- service linkage definition file 376
- service linkage execution information 19
- service linkage job 17
- service linkage job definition file
 - format 376
 - items 377
- Service linkage job definition window 148
 - Output definition file dialog box 150
- service linkage job information 17
- Service linkage job information definition files 361
- Service Linkage Job Log 240
- service linkage monitoring information 20
- service linkage monitoring job 17
- Service linkage monitoring job definition file 382
 - Format 382
 - Items 382
- Service linkage monitoring job definition window 151
- service linkage monitoring job information 17
- Service linkage monitoring job information definition files 378
- Service Linkage Monitoring Job Log 241
- Service linkage objects monitoring definition file 378
 - Format 378
 - Items 380
- service linkage objects monitoring information 20
- Service linkage objects monitoring job execution environment and permissions 134
- Setting
 - Setting up the JP1/AJS3 for Cloud Service Applications server 43
- Setting automatic startup and termination of the JP1/AJS3 for Cloud Service Applications service 56
- Setup 43
 - Cluster environment 50

- Execution host for a service linkage job 52
- Execution host for a service linkage monitoring job 52
- Service linkage jobs 43
- Service linkage monitoring jobs 43
- SSL communication environment 44
- Status of service linkage jobs 123
- storage
 - location of logs 237
- symbols used for command syntax explanations 203
- SYS_LOG_LANG 62
- SYS_LOG_LEVEL 62
- system configuration 22
- System property file for server management commands 78

T

- Timeout 84
- Troubleshooting 235
- Troubleshooting 258
- Troubleshooting for service linkage jobs 262
- Troubleshooting procedure 236
- Types and execution of service linkage monitoring jobs 128

U

- Uninstallation 41
 - Linux 41
 - Windows 41
- Unit definition parameters of service linkage jobs 116
- Unit definition parameters of service linkage monitoring jobs 118
- USED_DEF_LIMIT 68
- Use in cloud environment 28
- Use in on-premises environment 24
- User property file for J2EE server 74
- usrconf.cfg 76
- usrconf.properties 74, 78

V

- Variables used for the definition of service linkage job information 102
- Variables used for the definition of service linkage monitoring job information 103

W

- Web browser settings 144
- Window transitions 144

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
