

FUJITSU Software

Interstage Application Server

A decorative horizontal band with a red-to-dark-red gradient, featuring abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and energy.

Interstage HTTP Server 2.2

Operator's Guide

Windows/Solaris/Linux

B1WS-1118-02ENZ0(00)
April 2014

Preface

Purpose of this Document

This manual describes the environment setup and operation procedures required for Interstage HTTP Server 2.2 operation.

Intended Readers

It is assumed that readers of this document have some knowledge of the following:

- Basic knowledge of the OS used
- Basic knowledge about the Internet
- Basic knowledge about the Apache HTTP Server

Structure of This Document

This manual is organized as shown below:

[Chapter 1 Overview](#)

This chapter provides an overview of the functions provided in Interstage HTTP Server 2.2.

[Chapter 2 Functions](#)

This chapter describes the functions of Interstage HTTP Server 2.2.

[Chapter 3 Configuring the Web Server Operating Environment](#)

This chapter describes how to configure the Interstage HTTP Server 2.2 operating environment.

[Chapter 4 Operation and Maintenance](#)

This chapter describes the operation and maintenance of Interstage HTTP Server 2.2.

[Chapter 5 Tuning](#)

This chapter describes Interstage HTTP Server 2.2 tuning.

[Chapter 6 Directives](#)

This chapter describes directives that can be configured in Interstage HTTP Server 2.2.

[Chapter 7 Commands](#)

This chapter describes the Interstage HTTP Server 2.2 operation commands.

[Chapter 8 Messages](#)

This chapter describes the messages output by Interstage HTTP Server 2.2.

[Chapter 9 Troubleshooting](#)

This chapter describes the action to take if a problem occurs while Interstage HTTP Server 2.2 is running.

[Chapter 10 Migrating to Interstage HTTP Server 2.2](#)

This chapter describes Interstage HTTP Server 2.2 Migrating.

[Appendix A Miscellaneous Information](#)

This appendix describes miscellaneous Interstage HTTP Server 2.2 information.

[Appendix B Environment Variables and Server Variables](#)

This appendix describes the environment variables and server variables used in Interstage HTTP Server 2.2.

[Appendix C Setting the URL Rewrite](#)

This chapter describes how to set the URL rewrite.

Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of the Foreign Exchange and Foreign Trade Control Law of Japan and/or US export control laws.

Copyrights

Copyright 2013-2014 FUJITSU LIMITED

April 2014 Second Edition November 2013 First Edition
--

Contents

Chapter 1 Overview.....	1
1.1 Function Overview.....	1
1.2 Web Server Process Configuration (Windows(R)).....	1
1.3 Web Server Process Configuration (Solaris/Linux).....	3
Chapter 2 Functions.....	9
2.1 Number of Clients that can be Connected Simultaneously.....	9
2.2 Retrieving HTML Documents.....	9
2.3 Authentication and Access Control.....	10
2.3.1 User Authentication (Basic Authentication).....	11
2.3.2 IP Access Control.....	12
2.3.3 Client Authentication (Certificate Authentication).....	12
2.4 SSL.....	13
2.5 Virtual Host.....	14
2.6 Rewriting URLs.....	15
2.7 Server Status Monitoring.....	16
2.8 Multiple Web Servers.....	20
2.9 Compressing Content Function.....	21
2.10 Proxy Function.....	22
2.11 Timeout Value.....	23
2.12 Other Function.....	24
Chapter 3 Configuring the Web Server Operating Environment.....	27
3.1 Setting the Host Name.....	27
3.2 Setting the Document Root Directory.....	27
3.3 Setting the Port Number and IP Address.....	28
3.4 Setting the Access Log.....	29
3.5 Setting the Error Log.....	34
3.6 Setting the Trace Log.....	37
3.7 Setting User Authentication.....	41
3.8 Setting IP Access Control.....	44
3.9 Setting Client Authentication.....	47
3.10 Setting the SSL.....	51
3.10.1 SSL for Interstage Certificate Environments.....	51
3.10.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands.....	56
3.11 Setting the Virtual Host.....	63
3.12 Setting the Virtual Directory.....	67
3.13 Setting the Redirect Function.....	67
3.14 Setting the Rewrite Function.....	68
3.15 Setting the Server Status Monitoring.....	72
3.16 Setting the Compressing Content Function.....	73
3.17 Setting the Proxy Function.....	75
3.18 Setting the Directory List.....	77
3.19 Setting the Default MIME Type.....	77
3.20 Setting MIME Types.....	77
3.21 Setting the Default HTML File.....	78
3.22 Setting the HTTP Keep-Alive Function.....	78
3.23 Setting User tracking Function.....	79
3.24 Setting the Cookie Log.....	80
3.25 Setting the Privileges for the Communication Process.....	80
3.26 Setting Language-based Content Negotiation.....	81
3.27 Customizing the Messages.....	82
3.28 CGI Program Execution Permissions Settings.....	83
3.29 Access Control for Servlet Service Application URLs.....	85

Chapter 4 Operation and Maintenance.....	86
4.1 Starting and Stopping the Web Server.....	86
4.1.1 Starting the Web Server.....	86
4.1.2 Stopping the Web Server.....	87
4.1.3 Setting Auto Startup.....	88
4.1.4 Checking the Status.....	90
4.2 Log.....	90
4.2.1 Access Log.....	91
4.2.2 Error Log.....	93
4.2.3 Trace Log.....	94
4.3 Multiple Web Server Operation.....	97
4.3.1 Creating the Web Server Operating Environment.....	97
4.3.2 Deleting the Web Server Operating Environment.....	102
4.4 Maintenance (Resource Backup and Export).....	102
4.4.1 Backup and Export Procedure.....	103
4.4.2 Restore and Import Procedure.....	104
4.5 Cluster Service.....	104
4.5.1 Disabling the Interstage automatic startup setting.....	105
4.5.2 Interstage HTTP Server 2.2 Environment Setup.....	105
4.5.3 Setting the Cluster Service.....	105
4.5.4 Confirming the Cluster System Behavior.....	107
4.6 Security Measures.....	108
4.7 IPv6 Communication.....	111
4.8 Restrictions.....	111
4.9 Notes.....	111
Chapter 5 Tuning.....	114
5.1 Disk Space Requirements.....	114
5.2 Memory Requirements.....	114
5.3 System Resource Requirements (Solaris).....	114
5.4 System Resource Requirements (Linux).....	116
5.5 Environment Definition.....	118
5.5.1 Environment Definition File (httpd.conf).....	118
5.5.2 Web Server List File (servers.conf).....	119
Chapter 6 Directives.....	121
6.1 Notes on the Directives.....	130
6.2 Directives provided in Interstage HTTP Server 2.2.....	134
6.2.1 ISSsoBusinessSystemName.....	135
6.2.2 SSLCertExpand.....	136
6.2.3 SSLCertExpire.....	137
6.2.4 SSLCertName.....	138
6.2.5 SSLCipherSuite.....	138
6.2.6 SSLCICACertName.....	141
6.2.7 SSLConfName.....	141
6.2.8 SSLEnvDir.....	142
6.2.9 SSLExec.....	143
6.2.10 SSLHandshakeTimeout.....	143
6.2.11 SSLLIBMultiSession.....	144
6.2.12 SSLMaxSession.....	144
6.2.13 SSLNotifyVers.....	145
6.2.14 SSLSlotDir.....	146
6.2.15 SSLTokenLabel.....	146
6.2.16 SSLUserPINFile.....	147
6.2.17 SSLVerifyClient.....	147
6.2.18 SSLVersion.....	148
6.2.19 Trace.....	149
6.2.20 TraceLog.....	150

Chapter 7 Commands.....	152
7.1 ahsbackup.....	153
7.2 ahsrestore.....	155
7.3 ahslog.....	158
7.4 apachectl.....	164
7.5 htpasswd.....	165
7.6 httpd.....	167
7.7 ihsregistupin.....	169
Chapter 8 Messages.....	172
8.1 Messages Overview.....	172
8.1.1 Output Format.....	172
8.1.2 Before Contacting a Systems Engineer.....	173
8.2 ahs00000 to ahs00099.....	173
8.2.1 ahs00001.....	173
8.2.2 ahs00002.....	173
8.2.3 ahs00004.....	174
8.2.4 ahs00005.....	174
8.2.5 ahs00006.....	174
8.2.6 ahs00008.....	174
8.2.7 ahs00009.....	175
8.2.8 ahs00010.....	175
8.2.9 ahs00011.....	176
8.2.10 ahs00012.....	176
8.2.11 ahs00013.....	176
8.2.12 ahs00014.....	177
8.2.13 ahs00015.....	177
8.2.14 ahs00016.....	177
8.2.15 ahs00017.....	178
8.2.16 ahs00018.....	178
8.2.17 ahs00019.....	179
8.2.18 ahs00020.....	180
8.2.19 ahs00021.....	180
8.2.20 ahs00022.....	180
8.2.21 ahs00023.....	181
8.2.22 ahs00024.....	181
8.2.23 ahs00025.....	182
8.2.24 ahs00026.....	182
8.2.25 ahs00028.....	183
8.2.26 ahs00029.....	183
8.2.27 ahs00030.....	183
8.2.28 ahs00031.....	184
8.2.29 ahs00032.....	184
8.2.30 ahs00033.....	185
8.2.31 ahs00034.....	185
8.2.32 ahs00035.....	185
8.2.33 ahs00036.....	186
8.2.34 ahs00037.....	186
8.2.35 ahs00038.....	187
8.2.36 ahs00040.....	187
8.2.37 ahs00041.....	187
8.2.38 ahs00042.....	188
8.2.39 ahs00043.....	188
8.2.40 ahs00044.....	189
8.2.41 ahs00045.....	189
8.3 ahs00100 to ahs00199.....	189
8.3.1 ahs00100.....	189

8.3.2 ahs00101.....	190
8.3.3 ahs00102.....	190
8.3.4 ahs00103.....	191
8.3.5 ahs00104.....	191
8.3.6 ahs00105.....	191
8.3.7 ahs00106.....	192
8.3.8 ahs00107.....	192
8.3.9 ahs00108.....	193
8.3.10 ahs00109.....	193
8.3.11 ahs00111.....	193
8.3.12 ahs00112.....	194
8.3.13 ahs00113.....	194
8.3.14 ahs00114.....	194
8.3.15 ahs00115.....	195
8.3.16 ahs00116.....	195
8.3.17 ahs00117.....	196
8.3.18 ahs00118.....	196
8.3.19 ahs00119.....	196
8.3.20 ahs00120.....	197
8.3.21 ahs00123.....	197
8.3.22 ahs00124.....	197
8.3.23 ahs00125.....	198
8.3.24 ahs00126.....	198
8.3.25 ahs00127.....	198
8.3.26 ahs00128.....	199
8.3.27 ahs00129.....	199
8.3.28 ahs00130.....	200
8.3.29 ahs00131.....	200
8.3.30 ahs00132.....	200
8.3.31 ahs00133.....	201
8.3.32 ahs00134.....	201
8.3.33 ahs00135.....	201
8.3.34 ahs00136.....	202
8.3.35 ahs00137.....	202
8.3.36 ahs00138.....	202
8.3.37 ahs00139.....	203
8.3.38 ahs00140.....	203
8.3.39 ahs00141.....	203
8.3.40 ahs00142.....	204
8.4 ahs00200 to ahs00299.....	204
8.4.1 ahs00200.....	204
8.4.2 ahs00201.....	205
8.4.3 ahs00202.....	205
8.4.4 ahs00203.....	205
8.4.5 ahs00204.....	205
8.4.6 ahs00205.....	206
8.4.7 ahs00206.....	206
8.4.8 ahs00207.....	206
8.4.9 ahs00208.....	207
8.4.10 ahs00209.....	207
8.4.11 ahs00210.....	207
8.4.12 ahs00213.....	208
8.4.13 ahs00214.....	208
8.4.14 ahs00215.....	208
8.4.15 ahs00216.....	209
8.4.16 ahs00217.....	209
8.4.17 ahs00219.....	210

8.4.18 ahs00221.....	210
8.4.19 ahs00222.....	211
8.4.20 ahs00223.....	211
8.4.21 ahs00224.....	211
8.4.22 ahs00227.....	212
8.4.23 ahs00228.....	212
8.4.24 ahs00229.....	212
8.4.25 ahs00230.....	213
8.4.26 ahs00231.....	213
8.4.27 ahs00232.....	214
8.4.28 ahs00233.....	214
8.4.29 ahs00234.....	214
8.4.30 ahs00235.....	215
8.4.31 ahs00236.....	215
8.4.32 ahs00237.....	215
8.4.33 ahs00238.....	216
8.4.34 ahs00239.....	216
8.4.35 ahs00240.....	216
8.4.36 ahs00241.....	217
8.4.37 ahs00242.....	217
8.4.38 ahs00243.....	217
8.4.39 ahs00244.....	218
8.4.40 ahs00245.....	218
8.5 ahs00400 to ahs00499.....	219
8.5.1 ahs00401.....	219
8.5.2 ahs00402.....	219
8.5.3 ahs00403.....	220
8.6 ahs00500 to ahs00599.....	220
8.6.1 ahs00500.....	220
8.6.2 ahs00501.....	221
8.6.3 ahs00502.....	222
8.6.4 ahs00503.....	222
8.6.5 ahs00504.....	222
8.6.6 ahs00505.....	223
8.6.7 ahs00506.....	224
8.6.8 ahs00507.....	224
8.6.9 ahs00508.....	225
8.6.10 ahs00509.....	225
8.6.11 ahs00510.....	226
8.6.12 ahs00511.....	226
8.6.13 ahs00512.....	227
8.6.14 ahs00513.....	227
8.6.15 ahs00514.....	228
8.6.16 ahs00515.....	228
8.6.17 ahs00516.....	229
8.6.18 ahs00517.....	229
8.6.19 ahs00518.....	230
8.6.20 ahs00519.....	231
8.6.21 ahs00520.....	231
8.6.22 ahs00521.....	232
8.6.23 ahs00522.....	232
8.6.24 ahs00523.....	233
8.6.25 ahs00524.....	233
8.6.26 ahs00525.....	233
8.6.27 ahs00526.....	234
8.6.28 ahs00527.....	234
8.6.29 ahs00528.....	234

8.6.30 ahs00529.....	234
8.6.31 ahs00530.....	235
8.6.32 ahs00531.....	235
8.6.33 ahs00532.....	235
8.6.34 ahs00534.....	236
8.6.35 ahs00535.....	236
8.6.36 ahs00536.....	237
8.6.37 ahs00537.....	237
8.6.38 ahs00538.....	238
8.6.39 ahs00539.....	238
8.6.40 ahs00540.....	239
8.6.41 ahs00599.....	239
8.7 ahs70000 to ahs70099.....	239
8.7.1 ahs70004.....	239
8.7.2 ahs70005.....	240
8.7.3 ahs70007.....	240
8.7.4 ahs70008.....	240
8.7.5 ahs70009.....	240
8.8 ahs81000 to ahs81099.....	241
8.8.1 ahs81001.....	241
8.8.2 ahs81002.....	241
8.8.3 ahs81003.....	241
8.9 ahs81400 to ahs81499.....	242
8.9.1 ahs81400.....	242
8.9.2 ahs81401.....	242
8.9.3 ahs81402.....	242
8.9.4 ahs81403.....	243
8.9.5 ahs81404.....	243
8.9.6 ahs81405.....	243
8.9.7 ahs81406.....	243
8.9.8 ahs81407.....	244
8.9.9 ahs81408.....	244
8.9.10 ahs81409.....	244
8.9.11 ahs81410.....	244
8.9.12 ahs81411.....	244
8.9.13 ahs81412.....	245
8.9.14 ahs81413.....	245
8.9.15 ahs81414.....	245
8.9.16 ahs81415.....	246
8.9.17 ahs81416.....	246
8.9.18 ahs81417.....	246
8.9.19 ahs81418.....	247
8.9.20 ahs81419.....	247
8.9.21 ahs81420.....	247
8.9.22 ahs81421.....	248
8.9.23 ahs81422.....	248
8.9.24 ahs81423.....	249
8.9.25 ahs81424.....	249
8.9.26 ahs81425.....	249
8.9.27 ahs81426.....	250
8.9.28 ahs81427.....	250
8.9.29 ahs81428.....	251
8.9.30 ahs81429.....	251
8.9.31 ahs81430.....	252
8.9.32 ahs81431.....	252
8.9.33 ahs81432.....	252
8.9.34 ahs81433.....	253

8.9.35 ahs81434.....	253
8.9.36 ahs81435.....	253
8.9.37 ahs81439.....	254
8.9.38 ahs81440.....	254
8.9.39 ahs81451.....	255
8.9.40 ahs81452.....	255
8.9.41 ahs81453.....	255
8.10 Error Log.....	256
8.10.1 Messages Whose Log Levels are "emerg".....	257
8.10.2 Messages Whose Log Levels are "alert".....	260
8.10.3 Messages Whose Log Levels are "crit".....	267
8.10.4 Messages Whose Log Levels are "error".....	288
8.10.5 Messages Whose Log Levels are "warn".....	343
8.10.6 Messages Whose Log Levels are "notice".....	355
Chapter 9 Troubleshooting.....	362
9.1 Errors when the Web Server Starts or Stops.....	362
9.2 Errors During Web Server Operation.....	362
9.3 Errors When Multiple Web Servers are Used.....	365
9.4 Errors When the Cluster Service Function is Used.....	367
9.5 Frequently Asked Questions and Solutions.....	367
Chapter 10 Migrating to Interstage HTTP Server 2.2.....	369
Appendix A Miscellaneous Information.....	370
A.1 Log Files.....	370
A.2 Port Numbers.....	372
A.3 Resident Processes.....	373
A.4 Messages.....	374
A.4.1 Event Log.....	374
A.4.2 syslog.....	375
Appendix B Environment Variables and Server Variables.....	376
Appendix C Setting the URL Rewrite.....	385
C.1 Relating Directives.....	395
C.1.1 RewriteCond.....	396
C.1.2 RewriteEngine.....	397
C.1.3 RewriteRule.....	398

Chapter 1 Overview

This chapter provides an overview of the functions provided in Interstage HTTP Server 2.2.

1.1 Function Overview

Interstage HTTP Server 2.2 is a web server based on Apache HTTP Server Version 2.2.22.

In addition to the basic functions provided through Apache HTTP Server Version 2.2.22, the following functions are supported to meet various functional requirements on web servers:

- SSL
- Log file rotation function
- Trace log
- Cluster service
- Backup/restore



See

- Refer to Apache HTTP Server Version 2.2 Documentation for details on the Apache functions available when using Interstage HTTP Server 2.2. This documentation is contained in "ApplicationServer\apache\httpd-docs-2.2.22.en.zip". Extract this file, open folder "httpd-docs-2.2.22.en", and then open index.html.
- Refer to "[Chapter 6 Directives](#)" for details on the directives configured in the Interstage HTTP Server 2.2 environment configuration file (httpd.conf).



Note

The fix for the security hole detected in Apache HTTP Server Version 2.2 that affects Interstage HTTP Server 2.2 is effective for versions up to Apache HTTP Server Version 2.2.25. Additionally, if a problem related to a security hole occurs after this product is shipped, it will be fixed as needed by an urgent patch.

Security information on Fujitsu products is available from the following site. Keep checking the latest information.

<http://www.fujitsu.com/global/support/software/security/>

1.2 Web Server Process Configuration (Windows(R))

Windows32/64

Concurrent connection with clients is realized by using thread concurrency.

Interstage HTTP Server 2.2 threads are configured in the environment definition file (httpd.conf) using the following directives:

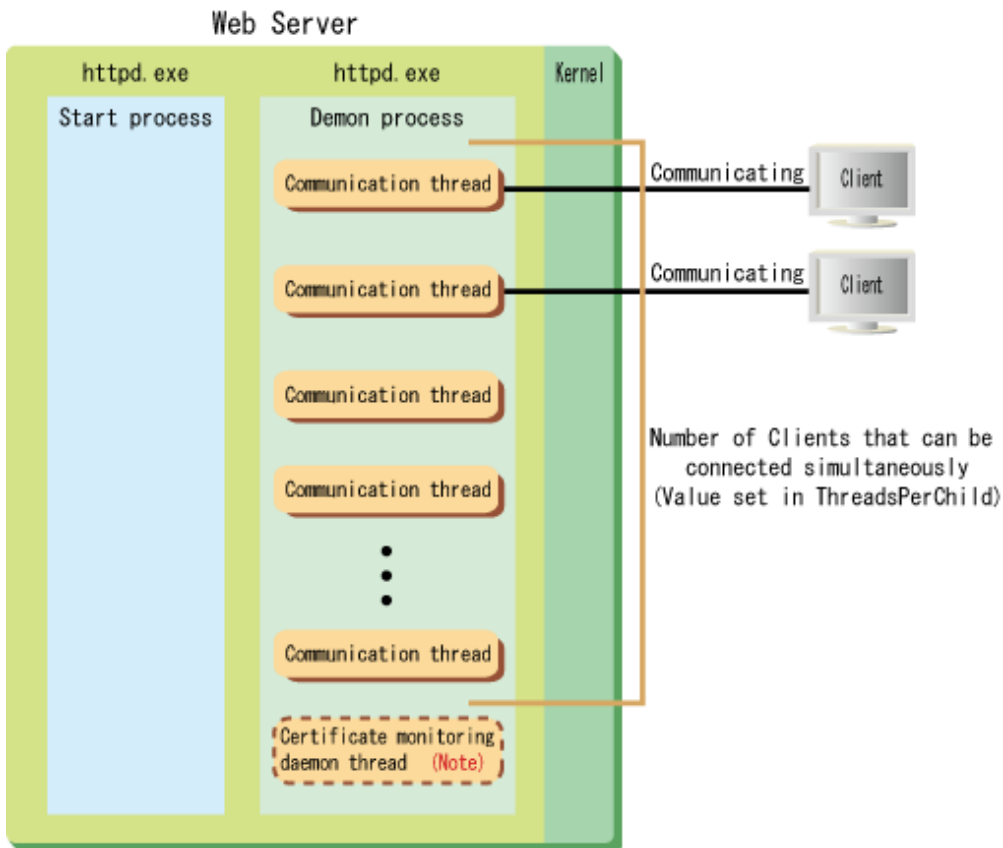
Description	Directive	Initial value
Number of clients that can be connected simultaneously	ThreadsPerChild	50
Number of requests that can be processed by the daemon process	MaxRequestsPerChild	0

The following sections describe how the values set in these directives affect the behavior of communication processes and threads:

- [Process configuration when the web server is started](#)
- [Maximum concurrency behavior](#)
- [Number of requests that can be processed by the daemon process](#)

Process configuration when the web server is started

When the web server is started, the daemon process creates the number of communication threads specified in the `ThreadsPerChild` directive. The number of communication threads does not increase or decrease, even when requests are received from the client, or when communication is broken.

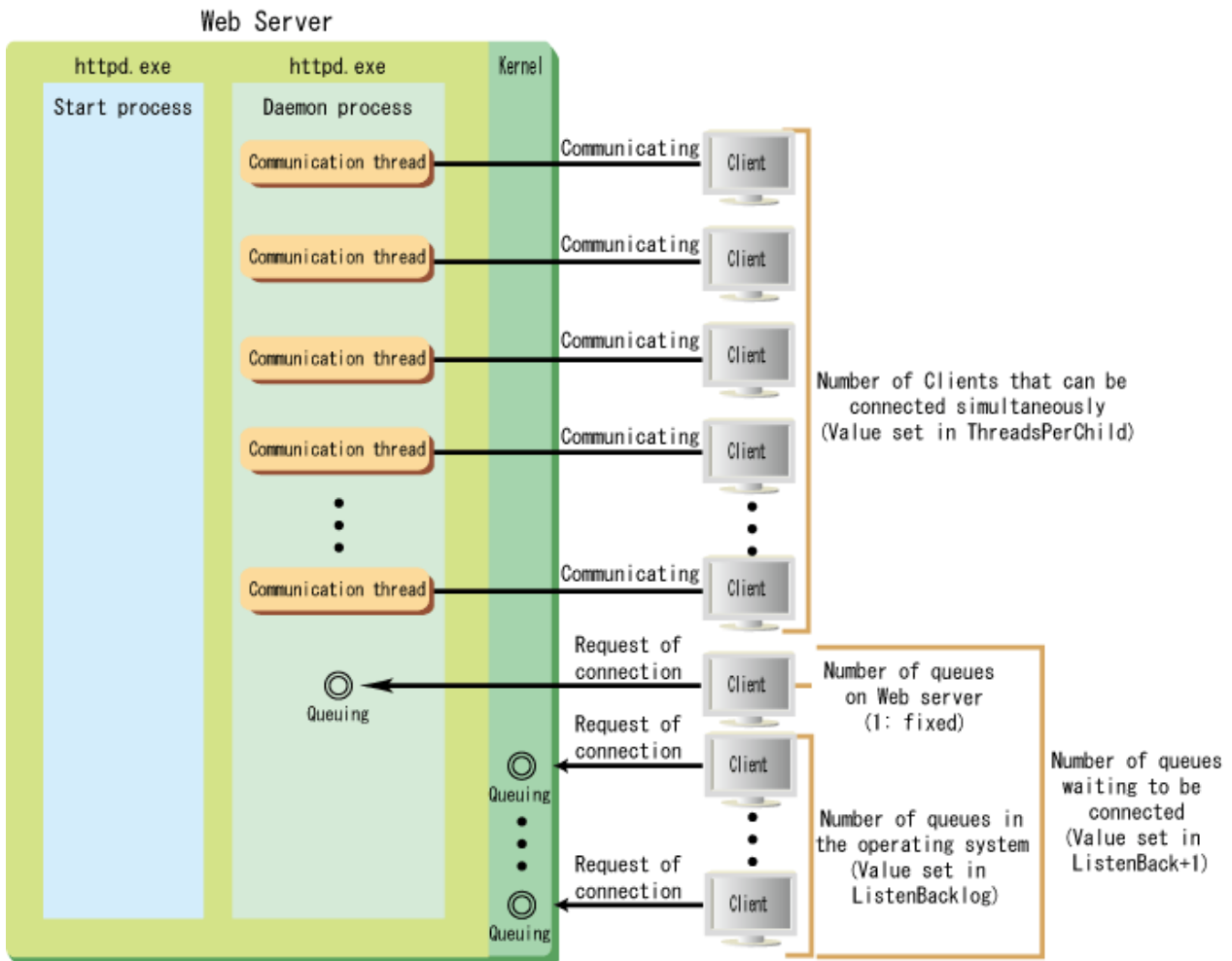


Note) The certificate monitoring daemon thread is created when the setting is configured to output a warning message that notifies the number of days the certificate is still valid during SSL operation on the web server. You may specify for the warning message to be output or not by configuring the [SSLCertExpire](#) directive.

Maximum concurrency behavior

If the number of concurrent connections with the client reaches the value set in the `ThreadsPerChild` directive, new requests from the client are placed in a queue on the web server and in the operating system.

There is one (fixed) queue on the web server. The number of queues in the operating system is set to the maximum number of queues specified in the `ListenBacklog` directive.



Number of requests that can be processed by the daemon process

If the total number of requests received after the daemon process is created exceeds the value set in the MaxRequestsPerChild directive, restart the daemon process. At this time, after the communication thread returns a response to the client and breaks the connection, the daemon process will end automatically.

1.3 Web Server Process Configuration (Solaris/Linux)

Solaris32/64 **Linux32/64**

Concurrent connection with clients is realized by using process/thread concurrency, and a feature that extends/degenerates the number of communication processes automatically is included.

Interstage HTTP Server 2.2 processes and threads are configured in the environment definition file (httpd.conf) using the following directives:

Description	Directive	Initial value
Process number when the web server is started	StartServers	5
Maximum value that can be set in "MaxClients / ThreadsPerChild (Note 1)"	ServerLimit	50
Number of clients that can be connected simultaneously	MaxClients	50
Minimum value for the number of communication threads in a wait state	MinSpareThreads	5

Description	Directive	Initial value
Maximum value for the number of communication threads in a wait state	MaxSpareThreads	10
Maximum value that can be set in ThreadsPerChild	ThreadLimit	- (Default value: 25)
Number of communication threads per communication process	ThreadsPerChild	1 (Note 2)
Number of requests that can be processed by one communication process	MaxRequestsPerChild	0

Note 1) "MaxClients / ThreadsPerChild" is the upper limit for the number of communication processes. Only the integer part of the calculation result is used.

Note 2) If linking with the web server connector, set the value of this directive to "1". The behavior of the web server cannot be guaranteed if a value other than "1" is set.

Point

Set the directives above according to the following rules.

ThreadsPerChild and ThreadLimit

```
ThreadsPerChild <= ThreadLimit
```

StartServers, ServerLimit, MaxClients, and ThreadsPerChild

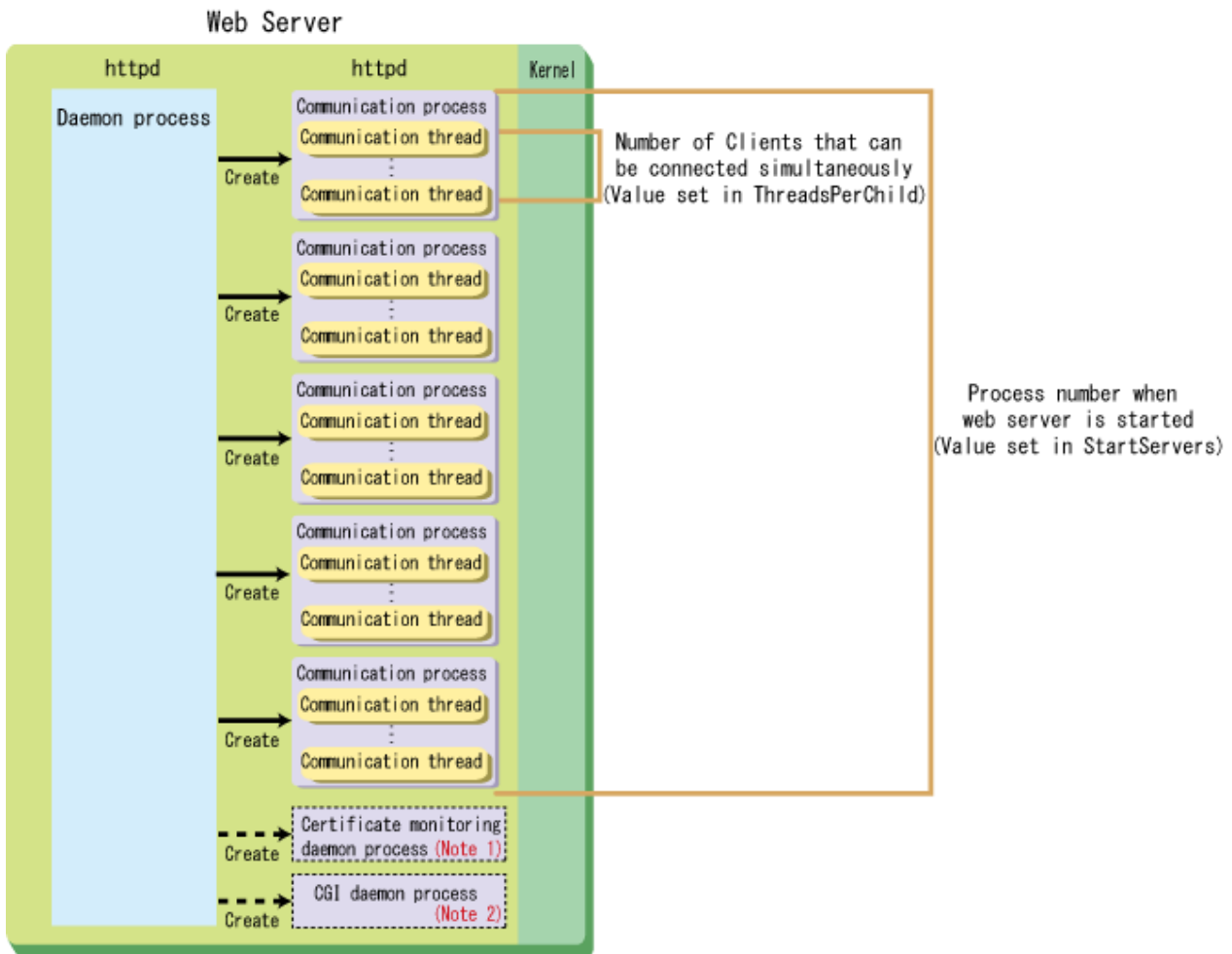
```
StartServers <= ( MaxClients / ThreadsPerChild ) <= ServerLimit
```

The following sections describe how the values set in the directives above affect the behavior of communication processes and threads:

- [Process configuration when the web server is started](#)
- [Extending the number of communication processes](#)
- [Degenerating the number of communication processes](#)
- [Maximum concurrency behavior](#)
- [Number of requests that can be processed by one communication process](#)

Process configuration when the web server is started

When the web server is started, the daemon process creates the number of communication processes specified in the StartServers directive.



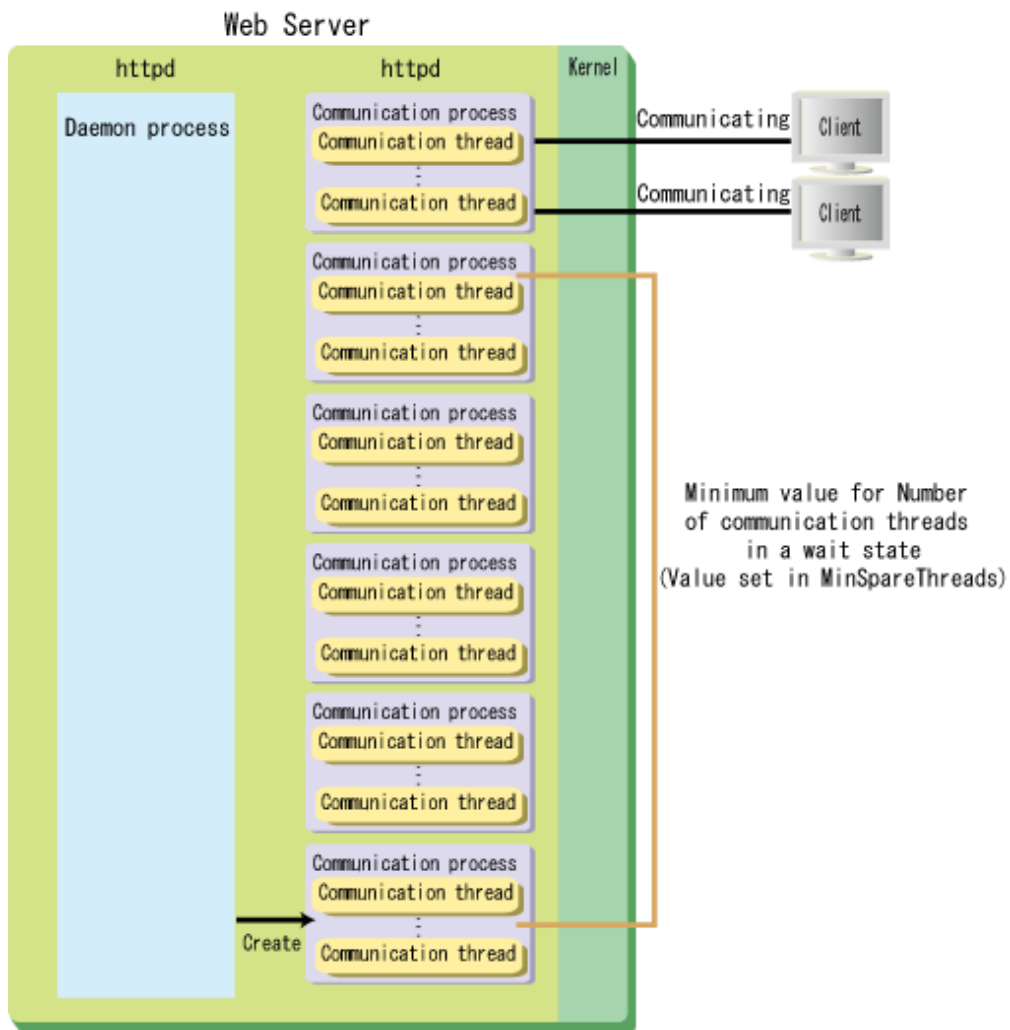
Note 1) The certificate monitoring daemon process is created when the setting is configured to output a warning message that notifies the number of days the certificate is still valid during SSL operation on the web server. You may specify for the warning message to be output or not by configuring the [SSLCertExpire](#) directive.

Note 2) The CGI daemon process is created during the CGI operation.

Extending the number of communication processes

When a connection request is received from the client, the communication threads will change from a wait state to a running state.

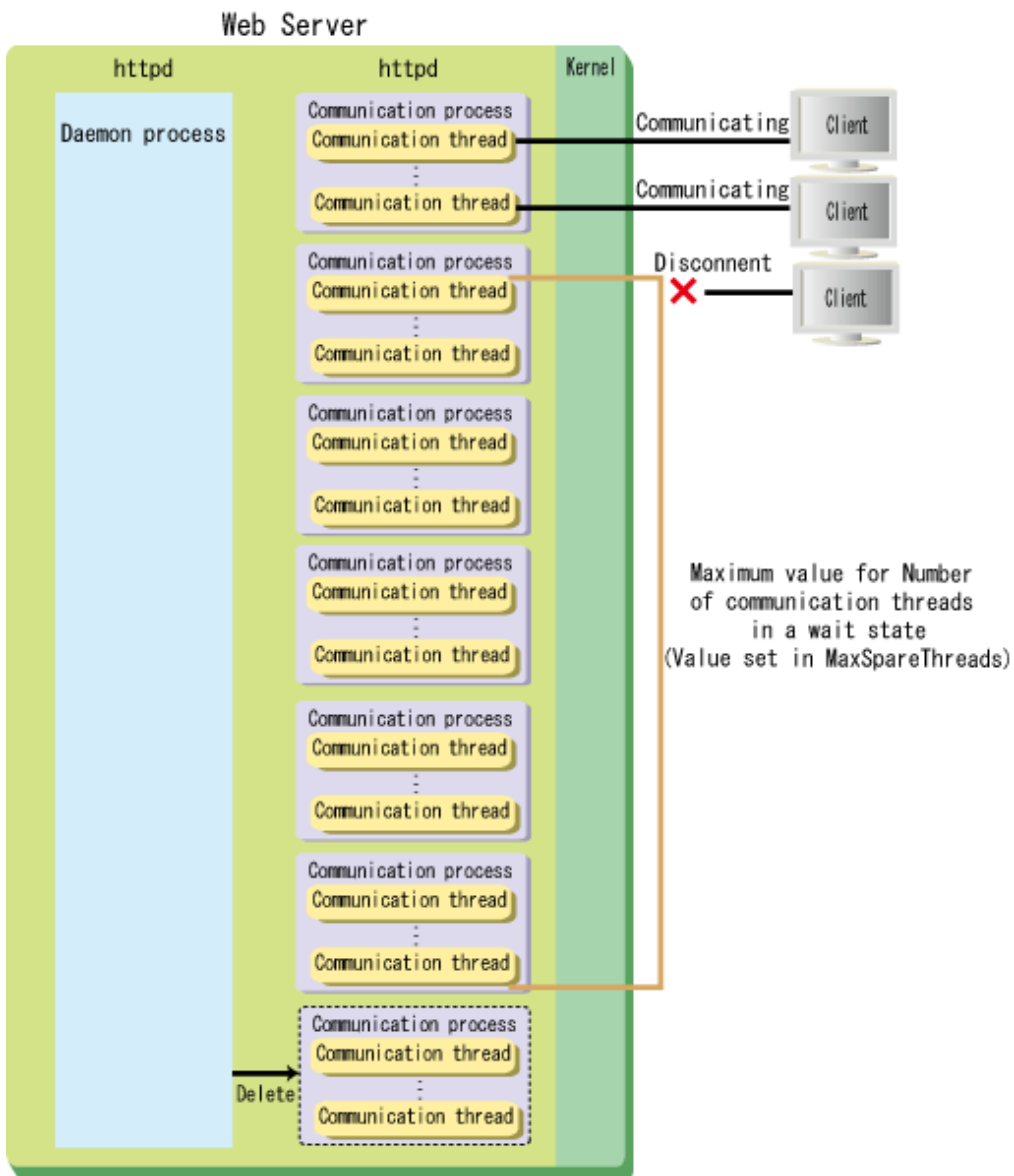
If the number of communication threads in a wait state is less than the value set in the `MinSpareThreads` directive, communication processes are created so that the number of threads is equal to or greater than the value set in the `MinSpareThreads` directive.



Degenerating the number of communication processes

If the connection with the client is broken, the communication threads will change to a wait state.

If the number of communication threads in a wait state exceeds the value set in the `MaxSpareThreads` directive, communication processes in a wait state are deleted so that the number of threads is equal to or less than the value set in the `MaxSpareThreads` directive.

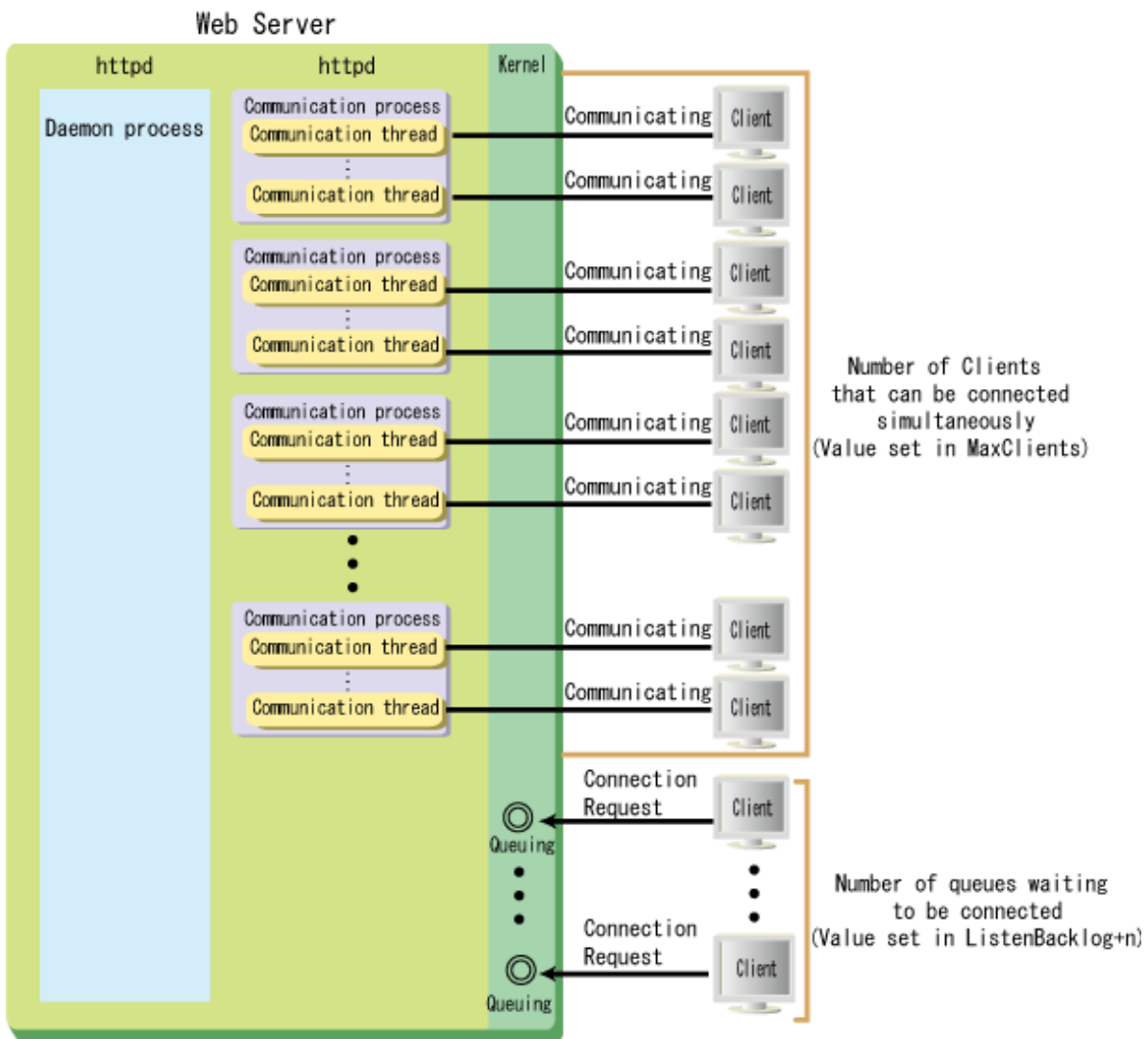


Maximum concurrency behavior

If the number of communication processes reaches the upper limit ($\text{MaxClients} / \text{ThreadsPerChild}$), new communication processes are not created.

Additionally, if the number of concurrent connections to the client reaches the value set in the `MaxClients` directive, new requests from the client are put in a queue in the operating system.

The number of queues in the operating system is set to the maximum number of queues specified in the `ListenBacklog` directive.



Note) n: Value corresponding to the specifications of the operating system

Number of requests that can be processed by one communication process

If the total number of requests received after the process is created exceeds the value set in the MaxRequestsPerChild directive for one communication process, restart that communication process. At this time, after the communication process returns a response to the client and breaks the connection, the communication process will end automatically.

Chapter 2 Functions

This chapter describes the functions of Interstage HTTP Server 2.2.

2.1 Number of Clients that can be Connected Simultaneously

In Interstage HTTP Server 2.2, the maximum number of concurrent requests that the web server can receive from the client (web browser) can be set.



Through this setting, the number of concurrent access requests will increase. Note, however, that overall system performance may degrade in line with increased consumption of memory resources and use of additional temporary files.



For details on the number of clients that can be connected simultaneously, refer to "[1.2 Web Server Process Configuration \(Windows\(R\)\)](#)" or "[1.3 Web Server Process Configuration \(Solaris/Linux\)](#)"

2.2 Retrieving HTML Documents

By specifying a URL in the web browser address bar, data (such as HTML pages and images) stored on the web server is retrieved and returned to the web browser.

The URL format specified in the web browser is shown below.

URL Synopsis

```
http://Host Name:Port Number/Path
```

Host Name

Name of the host on which the data is stored

Port Number

Port number

If the port number of the host is "80", it can be omitted (in this case, there is no need for a colon (":")).

Path

Path on the server to the requested resource

Searches the relative path from the DocumentRoot directive of the environment definition file (httpd.conf), and returns the content to the web browser.



- To use double-byte characters in URLs, configure the settings shown below. However, double-byte characters cannot be used in the query string in the URL.
 - In the web browser, enable the settings that send UTF-8 URLs.
Note If the settings that send UTF-8 URLs cannot be enabled, it will not be possible to send double-byte URLs.
 - **Solaris32/64** **Linux32/64**
On the web server, store HTML documents with file names that have "UTF-8" character encoding.

- In the initial settings, if the directory is specified without appending a slash ("/") to the URL path, processing by the web server will be as shown below.
 1. Status code "301" (Moved Permanently) is returned to the web browser (client). At this time, the redirect URL is set in the path to which the Host header value and slash ("/") are appended.
 2. A request to the redirect URL is received from the web browser (client).
 3. The file content set in the DirectoryIndex directive of the environment definition file (httpd.conf) is returned to the web browser (client).
- During installation, the sample content is stored in the directory specified in the DocumentRoot directive. Take the following action according to the web server operation:
 - Delete unnecessary sample content
 - Change the directory specified in the DocumentRoot directive

Example

Host Name	www.httpserver.com
Port Number	80
Document Root Directory	Windows32/64 C:\Interstage\F3FMahs\htdocs
	Solaris32/64 Linux32/64 /opt/FJSVahs\htdocs
HTML file	Windows32/64 C:\Interstage\F3FMahs\htdocs\index.html (Note)
	Solaris32/64 Linux32/64 /opt/FJSVahs\htdocs/index.html (Note)

Note) For sample content stored during installation, the following is displayed:

It works!

When the above operation is performed, the URL from the DocumentRoot directive of the environment definition file (httpd.conf) and web browser is specified as shown below.

If port number "80" is specified in the Listen directive of the environment definition file (httpd.conf), it can be omitted (when the installation is performed).

Value set for the DocumentRoot directive	Windows32/64 DocumentRoot "C:/Interstage/F3FMahs\htdocs"
	Solaris32/64 Linux32/64 DocumentRoot "/opt/FJSVahs\htdocs"
URL specified from the web browser	http://www.httpserver.com

2.3 Authentication and Access Control

There are three types of authentication, as shown below.

- [User Authentication \(Basic Authentication\)](#)
- [IP Access Control](#)

- Client Authentication (Certificate Authentication)

Point

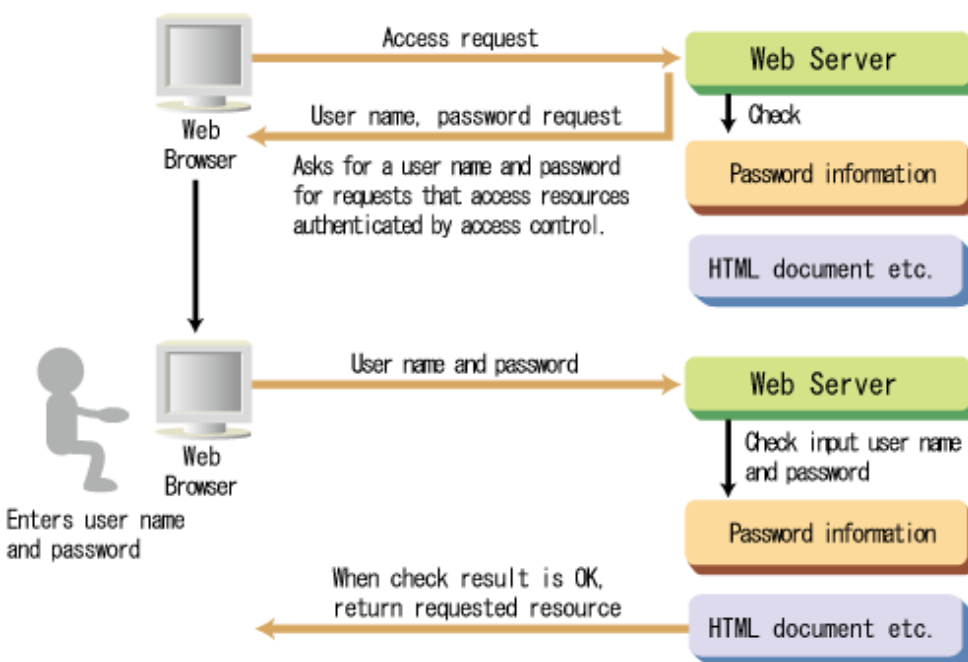
User authentication, IP access control, and client authentication can be used independently or together.

2.3.1 User Authentication (Basic Authentication)

User authentication allows or denies access to resources on the web server for each user by checking if user names and passwords are registered in the password file.

The web server determines whether or not to permit access to the resource from user names and passwords entered in the web browser.

The following figure shows how user authentication works.



Point

- In user authentication, the user name and password sent over the network are not encrypted, and therefore might be easily deciphered. To avoid this, use SSL for communication between the client and server to encrypt the user name and password and achieve a secure communication.
- Web server user authentication (basic authentication) information can be used in the web application.

See

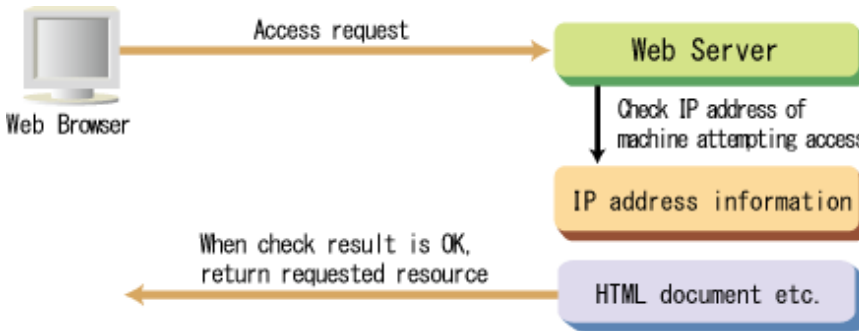
For details on settings, refer to "3.7 Setting User Authentication".

2.3.2 IP Access Control

IP access control limits accessing the resource on the web server for each IP address of the equipment in the access source.

Web server determines whether or not to permit access to the resource from the IP address of the machine that is attempting access.

The following figure shows how IP access control works.



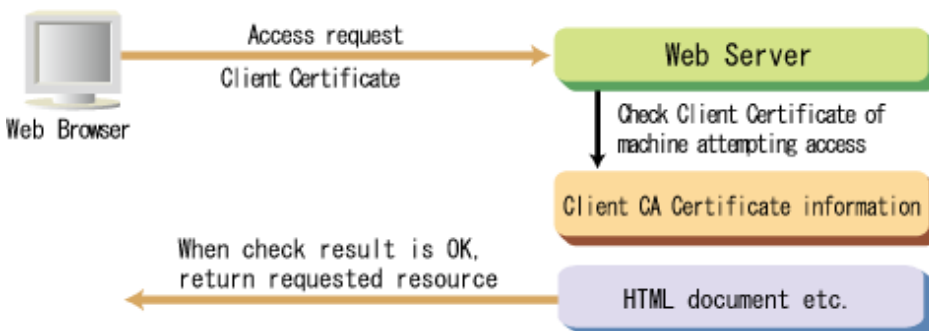
See

For details on settings, refer to "3.8 Setting IP Access Control".

2.3.3 Client Authentication (Certificate Authentication)

Client authentication restricts access to resources on the web server to users possessing a client certificate. As a result, the identity of the client (web browser) can be guaranteed.

The following figure shows how client authentication works.



Point

Use SSL protocol version SSL3.0 or SSL3.1 (TLS 1.0) for access restriction during client authentication.



See

For details on settings, refer to "3.9 Setting Client Authentication".

2.4 SSL

In Interstage HTTP Server 2.2, using client and server authentication and encrypted communication through SSL (Secure Sockets Layer) as the communication protocol between the web browser and the web server, security threats such as eavesdropping, tampering, and spoofing can be avoided, and the privacy of information can be maintained.

The URL format specified from the web browser when SSL operations are performed is shown below.

URL Synopsis

If access is performed using a URL that starts with "https", secure communication is performed automatically using the SSL protocol. This enables the safe transmission of what may be highly sensitive information.

```
https://Host Name:Port Number/Path
```

Host Name

Name of the host on which the data is stored

Port Number

Port number

If the port number of the host that uses SSL is "443", it can be omitted (in this case, there is no need for a colon (":")).

Path

Path on the server to the requested resource

Searches the relative path from the DocumentRoot directive of the environment definition file (httpd.conf), and returns the content to the web browser.

When performing SSL operations, one of the following environments must be built to manage the certificate and private key that are required for encryption and signature processing:

- Interstage certificate environment
- Certificate/key management environment configured with the SMEE command



See

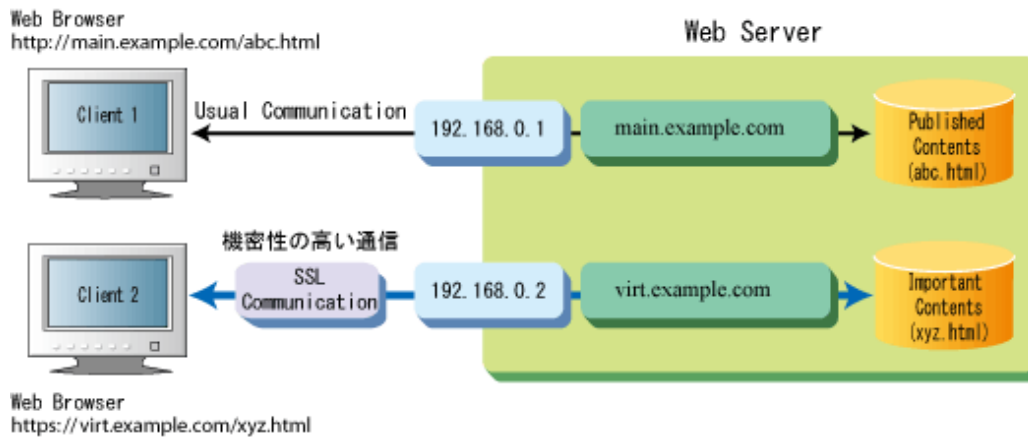
.....
For details on settings, refer to "3.10 Setting the SSL".
.....



Point

-
- When performing SSL operations, the CPU load caused by the processing of cryptographic algorithm calculations in the web server program will be heavy, therefore the communication processing performance may be affected. To accelerate the communication processing when performing SSL operations, install an SSL accelerator.

- In SSL, by performing operations together with a virtual host, information may be published using SSL and not using SSL at the same time.



2.5 Virtual Host

In Interstage HTTP Server 2.2, multiple virtual machines can be used from the web browser by operating web servers with a different host name (IP address/port number) on the same server machine.

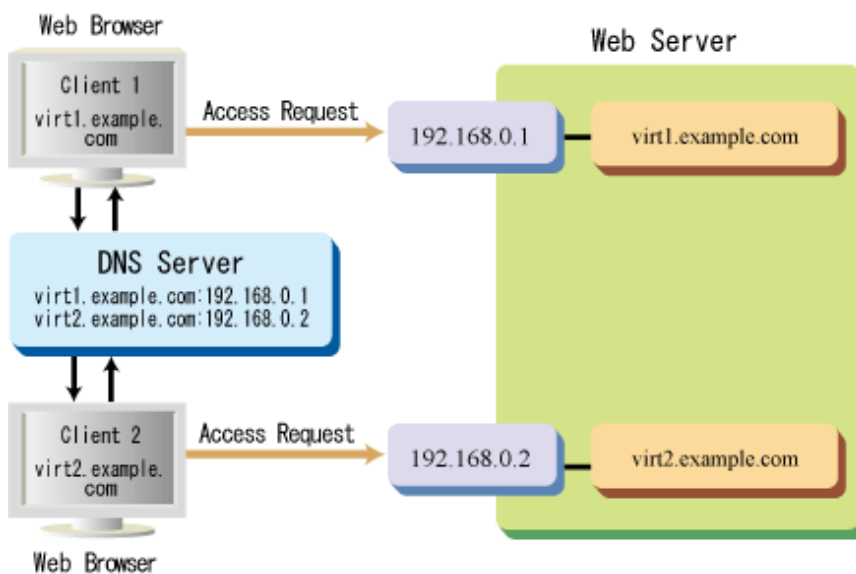
Using virtual hosting, a new host environment can be built without increasing the number of actual machines, so capital expenditure and operating costs can be kept under control.

There are two virtual host operation types:

- [IP and Port number-based virtual hosts](#)
- [Name-based virtual hosts](#)

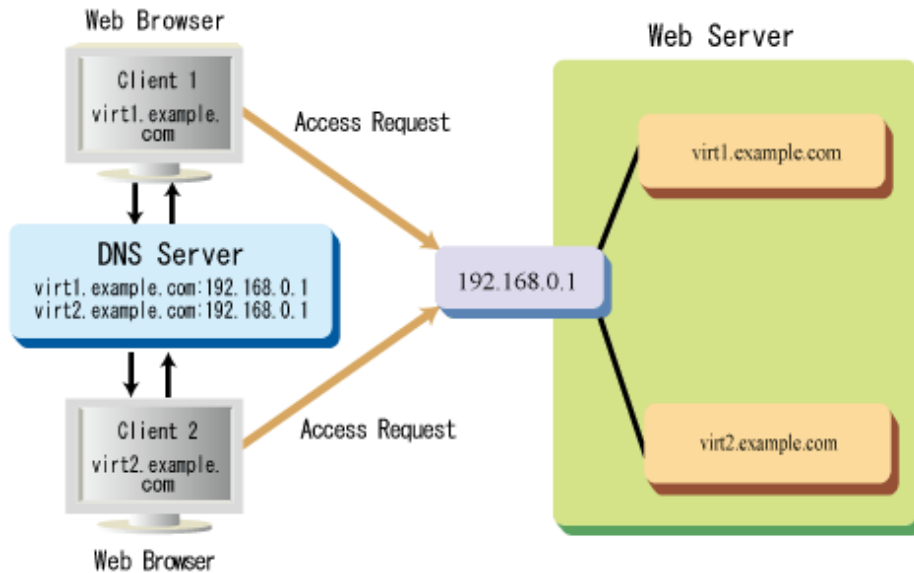
IP and port number-based virtual hosts

IP and port number-based virtual hosting sets multiple IP addresses and port numbers so that a virtual host is realized for each IP address and port number.



Name-based virtual hosts

Name-based virtual hosting assigns multiple host names to one IP address so that a virtual host is realized for each host name.



Note

- When using name-based virtual hosting, the load is concentrated on one actual machine, so this type of virtual hosting is not recommended if the emphasis is on performance. Consider access frequency and other such factors before using this type of hosting.
- SSL cannot be used if the name-based virtual host is set.

See

For details on setting, refer to "[3.11 Setting the Virtual Host](#)".

2.6 Rewriting URLs

In Interstage HTTP Server 2.2, the resources under the directory specified in the DocumentRoot directive of the environment definition file (httpd.conf) are normally accessed according to the URL specified from the client (web browser). However, it is possible to rewrite the URL using the following functions:

- [Virtual directory](#)
- [Redirect function](#)
- [Rewrite function](#)

Virtual directory

Using the virtual directory function, any directory may be assigned to a virtual path of a URL. Accordingly, the data of other directories can be published in a URL that contains a virtual path. This function is used to store data in paths to directories other than those set in the DocumentRoot directive, and to hide the paths where data is stored from external sources.



See

For details on setting, refer to "[3.12 Setting the Virtual Directory](#)".

Redirect function

Using the redirect function, a URL is rewritten to a new URL. Accordingly, if a page that cannot be used on the web server is accessed from the client (web browser), it is shown explicitly that the specified page cannot be accessed, and the old URL can be rewritten to a new URL. Using this function, the URL displayed on the web browser is also rewritten to a new URL, unlike the virtual directory function.



See

For details on setting, refer to "[3.13 Setting the Redirect Function](#)".

Rewrite function

Using the rewrite function, the URL rewrite conditions and rules are set as regular expressions, and the URL requested from the client (web browser) is rewritten when the rewrite conditions and rules are satisfied. Using this function, external redirection can be executed, and proxy requests can be activated, in the rewritten URL.



See

For details on setting, refer to "[3.14 Setting the Rewrite Function](#)".



Point

There are various methods of setting the URL rewrite, depending on the conversion conditions. Set the URL rewrite according to the web server operation method. For detail on the overview of the converted type and setting of the converted type, refer to "[Appendix C Setting the URL Rewrite](#)".

2.7 Server Status Monitoring

In Interstage HTTP Server 2.2, operational status information for the web server, such as the number of accesses, data transfer volume, and communication thread status, can be displayed and checked.



Note

When the server status monitoring function is operated, web server performance may be degraded.

The display content, method of setting, and operational procedures are shown below.

Display content

In the server status monitoring function, the operational status of the following items is displayed:

- [Operational status of the entire web server](#)
- [List of statuses for communication threads](#)

- Operational statuses for each communication thread

Operational status of the entire web server

If the operational status of the entire web server is year "yyyy", it will be displayed as shown in the following example:

Example

```
Current Time: Thursday, 18-Jan-yyyy 18:06:08 JST
Restart Time: Thursday, 18-Jan-yyyy 18:05:17 JST
Parent Server Generation: 0
Server uptime: 51 seconds
Total accesses: 4 - Total Traffic: 10 kB
CPU Usage: u.01 s.05 cu0 cs0 - .118% CPU load
.0784 requests/sec - 200 B/second - 2560 B/request
1 requests currently being processed, 5 idle workers
```

The meaning of each item displayed above is shown below.

Item Name	Meaning	Remarks	
Server Version	Interstage HTTP Server 2.2 server version		
Server Built	Interstage HTTP Server 2.2 compile date/time		
Current Time	Current date/time		
Restart Time	Start date/time		
Parent Server Generation	Number of restarts		
Server uptime	Continuous working hours		
Total accesses	Total number of accesses from startup	(Note)	
Total Traffic	Total data transfer volume	(Note)	
Solaris32/64 Linux32/64 CPU Usage	u	CPU time used by the communication process (seconds)	(Note)
	s	CPU time used by the system for communication processes (seconds)	(Note)
	cu	CPU time used by child processes generated in CGI access (seconds)	(Note)
	cs	CPU time used by the system for child processes generated in CGI access (seconds)	(Note)
Solaris32/64 Linux32/64 CPU load	CPU usage (%)	(Note)	
requests/sec	Average number of requests per second	(Note)	
B/second	Average data transfer volume per second	(Note)	
B/request	Data transfer volume per request	(Note)	
requests currently being processed	Number of requests being processed		
idle workers	Number of communication threads in a wait state		

Note) This is displayed if the server status information extended display is performed (if the value set in the ExtendedStatus directive of the environment definition file (httpd.conf) is "On").

List of statuses for communication threads

The list of statuses for communication threads generated by the web server is displayed per key in communication thread number (Srv) order, as shown below. This display is called a "scoreboard".

Example

```

_____W.....
.....
.....
.....
.....

```

Scoreboard Key:
 " _ " Waiting for Connection, " S " Starting up, " R " Reading Request,
 " W " Sending Reply, " K " Keepalive (read), " D " DNS Lookup,
 " C " Closing connection, " L " Logging, " G " Gracefully finishing,
 " I " Idle cleanup of worker, " . " Open slot with no current process

In the above example, the communication threads have the following statuses:

- First to fifth communication threads: Waiting
- Sixth communication thread: Replying
- Seventh and subsequent communication threads: Not started

The scoreboard key that shows the communication thread status, and the meaning, are shown as follows:

Scoreboard Key	Meaning
" _ " Waiting for Connection	Waiting
Solaris32/64 Linux32/64 "S" Starting up	Creating communication thread
"R" Reading Request	Reading request
"W" Sending Reply	Replying to request
"K" Keepalive (read)	Keep-Alive connection in progress
"D" DNS Lookup	Searching host name using DNS
"C" Closing connection	Closing connection
"L" Logging	Reading log file
"G" Gracefully finishing	Not started
"I" Idle cleanup of worker	- (Note)
". " Open slot with no current process	Not started

Note) This is disabled in Interstage HTTP Server 2.2, because it is not supported.

Operational statuses for each communication thread

The operational statuses for each communication thread are shown below.

Example

```

Srv PID Acc M CPU SS Req Conn Child Slot Client VHost Request
0-0 686 0/3/3 _ 0.04 10 1 0.0 0.01 0.01 192.168.1.1 httpserver GET /server-status HTTP/1.1
5-0 691 1/1/1 W 0.02 0 0 2.8 0.00 0.00 192.168.1.2 httpserver GET /server-status HTTP/1.1

```

The meaning of each item displayed above is shown below.

Item Name		Meaning	Remarks
Srv (Child Server number - generation)		Communication thread number - Number of restarts	(Note)
PID (OS process ID)		Process ID of the communication process	
Acc (Number of accesses this connection / this child / this slot)	Number of accesses this connection	Number of accesses using the same connection	(Note)
	this child	Total number of accesses per communication thread	
	this slot	Total number of accesses per communication thread	
M (Mode of operation)		Communication thread status (refer to " List of statuses for communication threads ")	
Solaris32/64 Linux32/64 CPU (CPU usage, number of seconds)		CPU consumption time (seconds)	(Note)
SS (Seconds since beginning of most recent request)		Elapsed time since most recent request (seconds)	(Note)
Req (Milliseconds required to process most recent request)		Processing time of most recent request (milliseconds)	(Note)
Conn (Kilobytes transferred this connection)		Data transfer volume in the same connection (kilobytes)	(Note)
Child (Megabytes transferred this child)		Total data transfer volume per communication thread (megabytes)	(Note)
Slot (Total megabytes transferred this slot)		Total data transfer volume per communication thread (megabytes)	(Note)
Client		Client or proxy server IP address	(Note)
VHost		Host name of web server that received the most recent request	(Note)
Request		Content of most recent request	(Note)

Note) This is displayed if the server status information extended display is performed (if the value set in the ExtendedStatus directive of the environment definition file (httpd.conf) is "On").

Method of setting

The server status monitoring function is set in the environment definition file (httpd.conf).

For details on setting, refer to "[3.15 Setting the Server Status Monitoring](#)".

Note

When the server status monitoring function is operated, there is a threat that a malicious user (or machine) on the network will intercept and look at that server status. To mitigate this threat, use the settings shown below.

- Configure the settings shown below together to allow only identified access.
 - User authentication settings
The server status information is displayed for access by a specific administrator only.
 - IP access control settings
The server status information is displayed for access from a specific client only.
- The <Location> section URL settings are complex.
When the <Location> section is set using the server status monitoring function, the "server-status" string is generally used in the URL. For this reason, if the "server-status" string is set in the URL, the server status information may be displayed without careful consideration. Set a string other than "server-status" in the URL.

Operational procedure

When the server status monitoring function is operated, the operational statuses in the above display content are displayed by accessing any URL from the client using the web browser.

URL Synopsis

```
http://Host Name:Port Number/Path
```

Host Name

Name of the host on which the data is stored

Port Number

Port number

If the port number of the host is "80", it can be omitted (in this case, there is no need for a colon (":")).

Path

URL set for <Location> section of the environment definition file (httpd.conf).

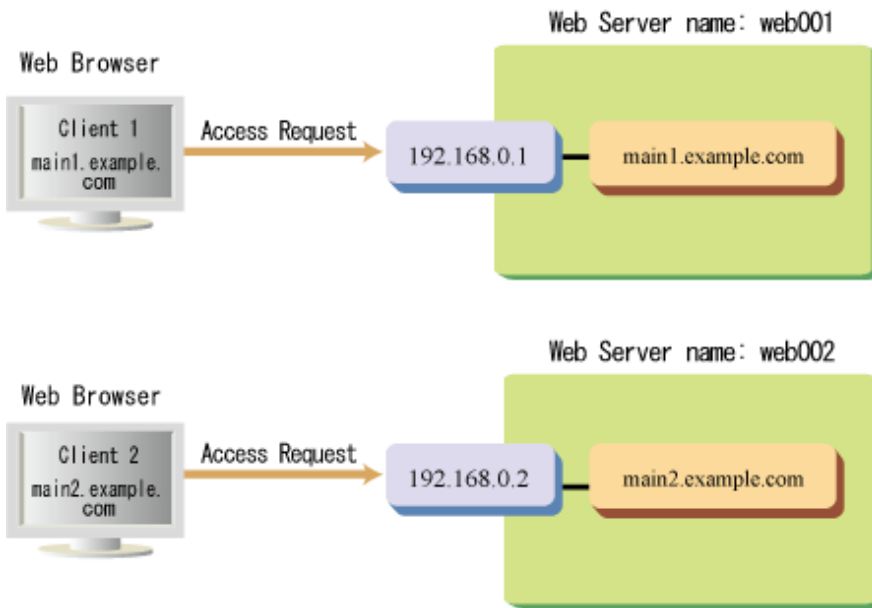
Point

- If "?auto" is specified at the end of the URL, a simplified status is displayed.
- If "?refresh=N" (N: Number of seconds) is specified at the end of the URL, the status display can be refreshed per the specified number of seconds. Note that, if "?refresh" is specified, the interval will be 10 seconds.

2.8 Multiple Web Servers

In Interstage HTTP Server 2.2, multiple web servers can be created and operated on a single system.

By using multiple web servers, flexible operations and minimization of the impact when a problem occurs can now be realized for each business operation.



See

For details on creating and deleting, refer to "4.3 Multiple Web Server Operation".

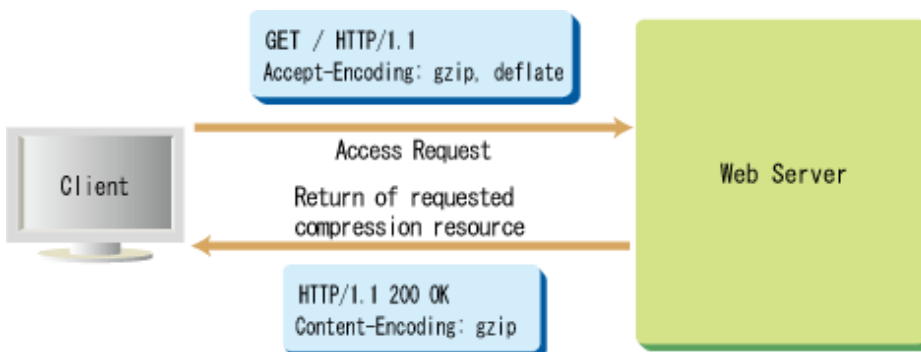
Note

To use one port number on multiple web servers, set a different "IP address:port number" for each web server before performing the operation. To use the same "IP address:port number", use the name-based virtual host function. For details on the virtual host, refer to "2.5 Virtual Host".

2.9 Compressing Content Function

In Interstage HTTP Server 2.2, the content that is sent to the client can be compressed.

Using this content compression function, the content transfer volume decreases, therefore the network load is reduced and the transfer efficiency of the request can be improved.



Note

If the content compression function is set, the value for the Content-Length header will be the size after the compression.



See

For details on setting, refer to "3.16 Setting the Compressing Content Function".

2.10 Proxy Function

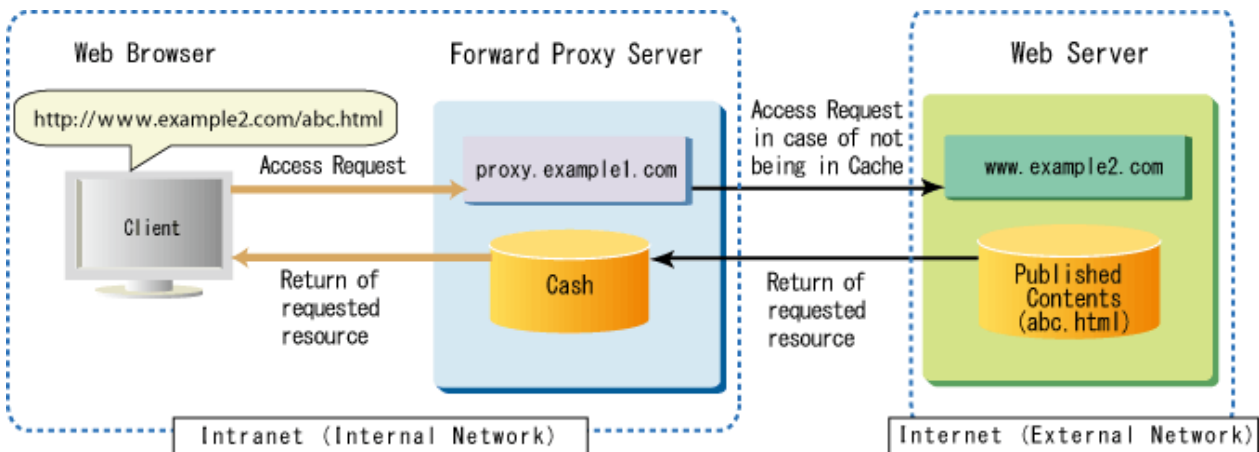
In Interstage HTTP Server 2.2, the following two proxy function types are provided:

- Forward proxy
- Reverse proxy

Forward proxy

The forward proxy is positioned on the client side between the client and the web server, and accesses the web server on behalf of the client request.

Generally, this function is used to allow access to external network web servers from an internal network client that is restricted by a firewall. Using a proxy server, the data from the web server can be saved in a cache.



See

For details on setting, refer to "Forward proxy" in "3.17 Setting the Proxy Function".



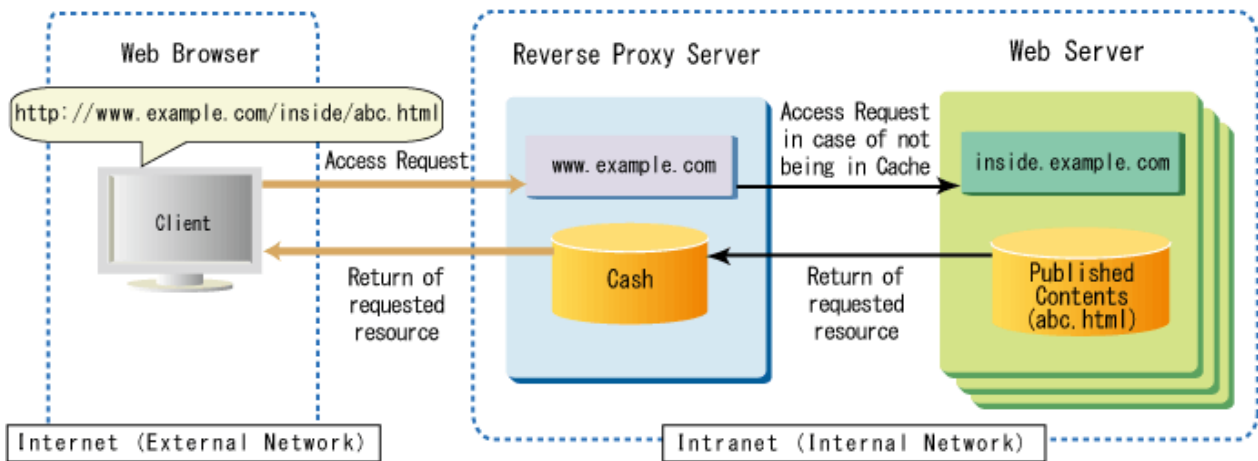
Note

To use the forward proxy function, configure the settings for using the proxy server on the web browser.

Reverse proxy

The reverse proxy is positioned on the web server side between the client and the web server, and receives the client request on behalf of the web server.

Generally, this function is used to access internal network web servers from an external network client by proxy. Using a proxy server, the data from the web server can be saved in a cache. Additionally, it can be used to show that one host is provided for content distributed to multiple hosts, for example.



See

For details on setting, refer to "Reverse proxy" in "3.17 Setting the Proxy Function".

Note

When the reverse proxy function is used, SSL communication cannot be used between the reverse proxy server and the web server.

2.11 Timeout Value

In Interstage HTTP Server 2.2, the following timeouts can be set between the client (web browser) and the web server:

- Client send/receive timeout (seconds)
- Timeout unit next request (seconds)

Client send/receive timeout (seconds)

This is the maximum wait time when data packets are sent or received between the client (web browser) and the web server. The client send/receive timeout (seconds) is set in the Timeout directive of the environment definition file (httpd.conf).

The send/receive timeout when the SSL connection is established is set in the [SSLHandshakeTimeout](#) directive of the environment definition file (httpd.conf).

Point

If the packet cannot be received even though the client send/receive timeout has been reached, the TCP connection will be broken. If the network traffic during the connection increases, and the TCP connection is broken frequently, the number of disconnections can be decreased by increasing this timeout.

Timeout until next request (seconds)

This is the maximum time the connection is retained until the next request after the HTTP response is sent from the web server, if the HTTP Keep-Alive function is set and a persistent connection is performed between the client (web browser) and the web server.

Point

If the HTTP Keep-Alive function is not set, the connection will close whenever a request is completed and a new connection will open for the next request. However, by setting the HTTP Keep-Alive function, multiple requests can be used in the same connection, therefore the client response improves.

2.12 Other Function

In Interstage HTTP Server 2.2, in addition to the functions explained to this point, the following functions can also be set:

- [Setting the directory list](#)
- [Setting the default MIME type](#)
- [Setting MIME types](#)
- [Setting the default HTML file](#)
- [User tracking Function](#)
- [Setting the cookie log](#)
- [Setting the privileges for the communication process](#) Solaris32/64 Linux32/64
- [Language-based content negotiation](#)
- [Customizing the messages](#)
- [CGI program execution permissions](#)

Setting the directory list

If the file set as the default page does not exist on the web server, the directory list (directory content list) is generated and displayed automatically.

See

For details on setting, refer to "[3.18 Setting the Directory List](#)".

Setting the default MIME type

The MIME type is set for files on the web server without extensions or with indeterminate extensions.

See

For details on setting, refer to "[3.19 Setting the Default MIME Type](#)".

Setting MIME types

Any MIME type on the web server is bound to the specified extension.

See

For details on setting, refer to "[3.20 Setting MIME Types](#)".

Setting the default HTML file

If the file name is omitted, a file other than "index.html" is set as the displayed default HTML file.



.....
For details on setting, refer to "[3.21 Setting the Default HTML File](#)".
.....

User tracking Function

By recording the access history information from the client in the log file, you can keep track of user visits.



.....
For details on setting, refer to "[3.23 Setting User tracking Function](#)".
.....

Setting the cookie log

The values for the Cookie header set in the request and the Set-Cookie header set when the response is made are written to the log file.



.....
For details on setting, refer to "[3.24 Setting the Cookie Log](#)".
.....

Setting the privileges for the communication process Solaris32/64 Linux32/64

Access restriction is set per user/group for the communication process.



.....
For details on setting, refer to "[3.25 Setting the Privileges for the Communication Process](#)".
.....

Language-based content negotiation

The Multiviews function is enabled, and the file name extension is bound to the specified language.



.....
For details on setting, refer to "[3.26 Setting Language-based Content Negotiation](#)".
.....

Customizing the messages

Information related to access, for example IP address or host name, data transfer volume, and personal information about a user, on a client or proxy server, for example, is written to the log file in the specified format.

Note

If large amounts of information are recorded about sites which are accessed heavily, there may be insufficient disk space.

See

For details on setting, refer to "[3.27 Customizing the Messages](#)".

CGI program execution permissions

By enabling the execution of CGI programs according to the methods shown below, it is possible to activate a CGI program stored on a web server from the web browser.

- A CGI program directory is set, and a file stored under that directory is executed as the CGI program.
- A CGI program extension is set, and a file with that extension is executed as the CGI program.

See

For details on setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".

Chapter 3 Configuring the Web Server Operating Environment

Before operating the web server, configure the web server operating environment if needed by placing the appropriate directives (configuration options) in the environment definition file (httpd.conf). For details on the environment definition file (httpd.conf), refer to "5.5.1 Environment Definition File (httpd.conf)".

This chapter describes how to configure the Interstage HTTP Server 2.2 operating environment.

3.1 Setting the Host Name

The server host name or IP address, and port number are set using the ServerName directive. The host name/IP address and port number are used to create the redirect URL if the UseCanonicalName directive is set to "On".



Example

Setting the server host name to "main.example.com"

```
ServerName main.example.com
```



Note

IPv6 addresses cannot be specified in the ServerName directive.



Information

Related Directives

- ServerName
- UseCanonicalName

3.2 Setting the Document Root Directory

The public root directory (the directory used by httpd to provide the files) is set using the DocumentRoot directive.



Example

Windows32/64

Setting the public root directory to "C:\Interstage\F3FMahs\htdocs"

```
DocumentRoot "C:/Interstage/F3FMahs/htdocs"
```

Solaris32/64 **Linux32/64**

Setting the public root directory to "/opt/FJSVahs/htdocs"

```
DocumentRoot "/opt/FJSVahs/htdocs"
```

Note

- During installation, the sample content is stored under the directory configured in the DocumentRoot directive. Depending on the web server operation, either delete unnecessary sample content, or change the directory specified in the DocumentRoot directive.
- **Solaris32/64** **Linux32/64**
You can use the directory specified in the DocumentRoot directive as the mount point to the NFS server, however, it must always be possible to access the NFS server while the web server is running. Before starting the web server, ensure that the NFS server is running normally. Additionally, while the web server is running, do not perform operations that will prevent access to the NFS server (such as powering off the NFS server).

Information

Related Directives

- DocumentRoot

3.3 Setting the Port Number and IP Address

The port number and IP address that receive the connection request are set using the Listen directive.

Example

Setting the port number to "80"

```
Listen 80
```

Setting the IP address to "127.0.0.1" and port number to "80"

```
Listen 127.0.0.1:80
```

Setting the IPv6 address to "2001:db8::a00:20ff:fea7:ccea" and port number to "80"

```
Listen [2001:db8::a00:20ff:fea7:ccea]:80
```

Note

- IPv4-mapped addresses cannot be specified in the IP address specified in the Listen directive.
- **Windows32/64**
In Windows Server(R) 2003, IPv6 address link-local addresses cannot be specified in the IP address specified in the Listen directive. If a link-local address is specified, error message ahs00018 is output to the event log (application) and the web server will fail to start.
- **Linux32/64**
IPv6 address link-local addresses cannot be specified in the IP address specified in the Listen directive. If a link-local address is specified, error message ahs00018 is output to the event log (application) and the web server will fail to start.
- In the web server, the following port numbers are generally used:
 - HTTP (when SSL is not used): 80
 - HTTPS (when SSL is used): 443

All services on the system, including applications, must have different port numbers set.

Information

Related Directives

- Listen

3.4 Setting the Access Log

The log file output content, destination, and rotation type for the access log are set by specifying the `ahsrlog` executable statement or log file name in the `CustomLog` directive.

The following examples are shown:

- When access log file rotation is performed in units of time
- When access log file rotation is performed in units of date/time
- When access log file rotation is performed in units of days of the week/time
- When access log file rotation is performed in units of number of days
- When access log file rotation is performed in units of file size
- When the access log file does not output a specific request by using the filtering function

Note

- If log rotation is not used, you may run out of disk space. For that reason, we recommend using log rotation. If log rotation is used, the oldest log file is deleted and a new log file is created when the upper limit for the number of log files specified in the `ahsrlog` executable statement is reached.
- Do not specify the same log file in the main host and virtual host, or in a different directory. If multiple web servers are running, do not specify the same log file as another web server. If the same file name is specified, the log file content and the log rotation behavior cannot be guaranteed.
- During installation, a message is output by the `ahsrlog` specified in the `CustomLog` directive to the log file shown below. If necessary, the log file destination can be changed. However, if it is changed, the information cannot be collected using the batch information collection tool (`iscollectinfo` command), so you must collect the log files separately.

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\logs\accesslog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/accesslog
```

- **Solaris32/64** **Linux32/64**

The `"/opt/FJSVahs/logs/accesslog"` log file specified in the example below is a symbolic link file. If the `"/opt/FJSVahs/logs/accesslog"` symbolic link file is specified in the log file, the access log file will be stored under `/var/opt/FJSVahs/logs`.

Point

- By specifying the `ahsrlog` option in the log file output by specifying the `ahsrlog` executable statement, each log rotation can be specified as the following units:
 - Units of time (`-T` option)
 - Units of date/time (`-C` option)
 - Units of days of the week/time (`-W` option)

- Units of days (-d option)
- Units of file sizes (-s option)
- A filtering feature can be used. By using the SetEnvIf directive to set an environment variable based on the HTTP request attribute, the settings can be configured so that access logs such as requests from a specific IP address or requests to a specific URL will not be output.
- For details on output Items, refer to "4.2.1 Access Log".
- The settings can also be configured using the TransferLog directive.

When access log file rotation is performed in units of time

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog " | | \"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -T \"C:/Interstage/F3FMahs/logs/accesslog\"
0900,1700 5\" ahs-analysis
```

Solaris32/64 Linux32/64

When access log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog " | /opt/FJSVahs/bin/ahsrlog -T /opt/FJSVahs/logs/accesslog 0900,1700 5\" ahs-analysis
```

When access log file rotation is performed in units of date/time

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog " | | \"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -C \"C:/Interstage/F3FMahs/logs/accesslog\"
1,11,21 5\" ahs-analysis
```

Solaris32/64 Linux32/64

When access log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month

- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog " | /opt/FJSVahs/bin/ahsrlog -C /opt/FJSVahs/logs/accesslog 1,11,21 5" ahs-analysis
```

Note

For months not containing 31 days, rotating through log files will not be performed on the 31st, even if "31" is specified for the -C option. If you want rotating through log files to be performed at the end of the month, investigate setting rotating through log files to be performed at 00hh 00mm on the 1st.

When access log file rotation is performed in units of days of the week/time

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog " | |\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -W \"C:/Interstage/F3FMahs/logs/accesslog\" Mon,Sat 5" ahs-analysis
```

Solaris32/64 Linux32/64

When access log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog " | /opt/FJSVahs/bin/ahsrlog -W /opt/FJSVahs/logs/accesslog Mon,Sat 5" ahs-analysis
```

When access log file rotation is performed in units of number of days

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -d \"C:/Interstage/F3FMahs/logs/accesslog\" 1 5" ahs-analysis
```

Solaris32/64 **Linux32/64**

When access log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -d /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis
```

When access log file rotation is performed in units of file size

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- File Size: 1 MB
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/accesslog\" 1 5" ahs-analysis
```

Solaris32/64 **Linux32/64**

When access log file rotation is performed according to the following conditions:

- File Size: 1 MB
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis
```

When the access log file does not output a specific request by using the filtering function

Example

Windows32/64

When access log file rotation is performed according to the following conditions:

- The request from IP address "192.168.1.1" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module "C:/Interstage/F3FMahs/modules/mod_setenvif.so"  
SetEnvIf Remote_Addr 192\.168\.1\.1 nolog_remote_addr  
CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/accesslog\" 1 5" ahs-analysis env=!nolog_remote_addr
```

When access log file rotation is performed according to the following conditions:

- The request to URL"/abc/" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module "C:/Interstage/F3FMahs/modules/mod_setenvif.so"
SetEnvIf Request_URI "^/abc/" nolog_request_uri
CustomLog "|\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/accesslog\"
1 5" ahs-analysis env=!nolog_request_uri
```

When access log file rotation is performed according to the following conditions:

- The request of method "HEAD" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module "C:/Interstage/F3FMahs/modules/mod_setenvif.so"
SetEnvIf Request_Method HEAD nolog_request_method
CustomLog "|\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/accesslog\"
1 5" ahs-analysis env=!nolog_request_method
```

Solaris32/64 **Linux32/64**

When access log file rotation is performed according to the following conditions:

- The request from IP address "192.168.1.1" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module /opt/FJSVahs/modules/mod_setenvif.so
SetEnvIf Remote_Addr 192\.168\.1\.1 nolog_remote_addr
CustomLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis env=!
nolog_remote_addr
```

When access log file rotation is performed according to the following conditions:

- The request to URL"/abc/" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module /opt/FJSVahs/modules/mod_setenvif.so
SetEnvIf Request_URI "^/abc/" nolog_request_uri
CustomLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis env=!
nolog_request_uri
```

When access log file rotation is performed according to the following conditions:

- The request of method "HEAD" is not output to the access log.
- The log file rotation is performed in units of file size.

```
LoadModule setenvif_module /opt/FJSVahs/modules/mod_setenvif.so
SetEnvIf Request_Method HEAD nolog_request_method
CustomLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis env=!
nolog_request_method
```

Information

Related Directives

- CustomLog
- LoadModule
- SetEnvIf

3.5 Setting the Error Log

The log file output content, destination, and rotation type for the error log are set by specifying the `ahsrlog` executable statement or log file name in the `ErrorLog` directive.

The following examples are shown:

- When error log file rotation is performed in units of time
- When error log file rotation is performed in units of date/time
- When error log file rotation is performed in units of days of the week/time
- When error log file rotation is performed in units of number of days
- When error log file rotation is performed in units of file size

Note

- If log rotation is not used, you may run out of disk space. For that reason, we recommend using log rotation. If log rotation is used, the oldest log file is deleted and a new log file is created when the upper limit for the number of log files specified in the `ahsrlog` executable statement is reached.
- Do not specify the same log file in the main host and virtual host, or in a different directory. If multiple web servers are running, do not specify the same log file as another web server. If the same file name is specified, the log file content and the log rotation behavior cannot be guaranteed.
- During installation, a message is output by the `ahsrlog` specified in the `ErrorLog` directive to the log file shown below. If necessary, the log file destination can be changed. However, if it is changed, the information cannot be collected using the batch information collection tool (`iscollectinfo` command), so you must collect the log files separately.

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\logs\errorlog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/errorlog
```

- If the `ErrorLog` directive is set more than once for the main host or virtual host, the most recent configuration for each will be used.
 - **Solaris32/64** **Linux32/64**
The `"/opt/FJSVahs/logs/errorlog"` log file specified in the example below is a symbolic link file. If the `"/opt/FJSVahs/logs/errorlog"` symbolic link file is specified in the log file, the error log file will be stored under `/var/opt/FJSVahs/logs`.
-

Point

- By specifying the `ahsrlog` option in the log file output by specifying the `ahsrlog` executable statement, each log rotation can be specified as the following units:
 - Units of time (`-T` option)
 - Units of date/time (`-C` option)
 - Units of days of the week/time (`-W` option)
 - Units of days (`-d` option)
 - Units of file sizes (`-s` option)
 - For details on output Items, refer to "[4.2.2 Error Log](#)".
-

When error log file rotation is performed in units of time



Example

Windows32/64

When error log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\errorlog
- File count upper limit: 5

```
ErrorLog " | |\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe" -T \\"C:/Interstage/F3FMahs/logs/errorlog\"  
0900,1700 5"
```

Solaris32/64 Linux32/64

When error log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: /var/opt/FJSVahs/logs/errorlog
- File count upper limit: 5

```
ErrorLog " | /opt/FJSVahs/bin/ahsrlog -T /opt/FJSVahs/logs/errorlog 0900,1700 5"
```

When error log file rotation is performed in units of date/time



Example

Windows32/64

When error log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\errorlog
- File count upper limit: 5

```
ErrorLog " | |\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe" -C \\"C:/Interstage/F3FMahs/logs/errorlog\"  
1,11,21 5"
```

Solaris32/64 Linux32/64

When error log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/errorlog
- File count upper limit: 5

```
ErrorLog " | /opt/FJSVahs/bin/ahsrlog -C /opt/FJSVahs/logs/errorlog 1,11,21 5"
```

Note

For months not containing 31 days, rotating through log files will not be performed on the 31st, even if "31" is specified for the -C option. If you want rotating through log files to be performed at the end of the month, investigate setting rotating through log files to be performed at 00hh 00mm on the 1st.

When error log file rotation is performed in units of days of the week/time

Example

Windows32/64

When error log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\errorlog
- File count upper limit: 5

```
ErrorLog " | |\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -W \\"C:/Interstage/F3FMahs/logs/errorlog\"  
Mon,Sat 5"
```

Solaris32/64 **Linux32/64**

When error log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/errorlog
- File count upper limit: 5

```
ErrorLog " | /opt/FJSVahs/bin/ahsrlog -W /opt/FJSVahs/logs/errorlog Mon,Sat 5"
```

When error log file rotation is performed in units of number of days

Example

Windows32/64

When error log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: C:\Interstage\F3FMahs\logs\errorlog
- File count upper limit: 5

```
ErrorLog " | |\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -d \\"C:/Interstage/F3FMahs/logs/errorlog\" 1 5"
```

Solaris32/64 **Linux32/64**

When error log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"

- File Name: /var/opt/FJSVahs/logs/errorlog
- File count upper limit: 5

```
ErrorLog "|/opt/FJSVahs/bin/ahsrlog -d /opt/FJSVahs/logs/errorlog 1 5"
```

When error log file rotation is performed in units of file size

Example

Windows32/64

When error log file rotation is performed according to the following conditions:

- File Size: 1 MB
- File Name: C:\Interstage\F3FMahs\logs\errorlog
- File count upper limit: 5

```
ErrorLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/errorlog\" 1 5"
```

Solaris32/64 **Linux32/64**

When error log file rotation is performed according to the following conditions:

- File Size: 1 MB
- File Name: /var/opt/FJSVahs/logs/errorlog
- File count upper limit: 5

```
ErrorLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/errorlog 1 5"
```

Information

Related Directives

- ErrorLog

3.6 Setting the Trace Log

The log file output content, destination, and rotation type for the error log are set by specifying the ahsrlog executable statement or log file name in the [TraceLog](#) directive.

The following examples are shown:

- [When trace log file rotation is performed in units of time](#)
- [When trace log file rotation is performed in units of date/time](#)
- [When trace log file rotation is performed in units of days of the week/time](#)
- [When trace log file rotation is performed in units of number of days](#)
- [When trace log file rotation is performed in units of file size](#)

Note

- To disable trace logging, set the Trace directive to "Off".

- If log rotation is not used, you may run out of disk space. For that reason, we recommend using log rotation. If log rotation is used, the oldest log file is deleted and a new log file is created when the upper limit for the number of log files specified in the ahrslog executable statement is reached.
- Do not specify the same log file in the main host and virtual host, or in a different directory. If multiple web servers are running, do not specify the same log file as another web server. If the same file name is specified, the log file content and the log rotation behavior cannot be guaranteed.
- During installation, a message is output by the ahrslog specified in the [TraceLog](#) directive to the log file shown below. If necessary, the log file destination can be changed. However, if it is changed, the information cannot be collected using the batch information collection tool (iscollectinfo command), so you must collect the log files separately.

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\logs\tracelog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/tracelog
```

- **Solaris32/64** **Linux32/64**
The "/opt/FJSVahs/logs/tracelog" log file specified in the example below is a symbolic link file. If the "/opt/FJSVahs/logs/tracelog" symbolic link file is specified in the log file, the trace log file will be stored under /var/opt/FJSVahs/logs.

Point

- By specifying the ahrslog option in the log file output by specifying the ahrslog executable statement, each log rotation can be specified as the following units:
 - Units of time (-T option)
 - Units of date/time (-C option)
 - Units of days of the week/time (-W option)
 - Units of days (-d option)
 - Units of file sizes (-s option)
- For details on output Items, refer to "[4.2.3 Trace Log](#)".

When trace log file rotation is performed in units of time

Example

Windows32/64

When trace log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  " || \"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -T \"C:/Interstage/F3FMahs/logs/tracelog\"
0900,1700 5"
```

Solaris32/64 **Linux32/64**

When trace log file rotation is performed according to the following conditions:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: /var/opt/FJSVahs/logs/tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  " | /opt/FJSVahs/bin/ahsrlog -T /opt/FJSVahs/logs/tracelog 0900,1700 5"
```

When trace log file rotation is performed in units of date/time

Example

Windows32/64

When trace log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  " | | \"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -C \"C:/Interstage/F3FMahs/logs/tracelog\"
1,11,21 5"
```

Solaris32/64 Linux32/64

When trace log file rotation is performed according to the following conditions:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  " | /opt/FJSVahs/bin/ahsrlog -C /opt/FJSVahs/logs/tracelog 1,11,21 5"
```

Note

For months not containing 31 days, rotating through log files will not be performed on the 31st, even if "31" is specified for the -C option. If you want rotating through log files to be performed at the end of the month, investigate setting rotating through log files to be performed at 00hh 00mm on the 1st.

When trace log file rotation is performed in units of days of the week/time

Example

Windows32/64

When trace log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm

- File Name: C:\Interstage\F3FMahs\logs\tracelog
- File count upper limit: 5

```
Trace    On
TraceLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -W \"C:/Interstage/F3FMahs/logs/tracelog\"
Mon,Sat 5"
```

Solaris32/64 **Linux32/64**

When trace log file rotation is performed according to the following conditions:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/tracelog
- File count upper limit: 5

```
Trace    On
TraceLog "||/opt/FJSVahs/bin/ahsrlog -W /opt/FJSVahs/logs/tracelog Mon,Sat 5"
```

When trace log file rotation is performed in units of number of days



Example

Windows32/64

When trace log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: C:\Interstage\F3FMahs\logs\tracelog
- File count upper limit: 5

```
Trace    On
TraceLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -d \"C:/Interstage/F3FMahs/logs/tracelog\" 1 5"
```

Solaris32/64 **Linux32/64**

When trace log file rotation is performed according to the following conditions:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: /var/opt/FJSVahs/logs/tracelog
- File count upper limit: 5

```
Trace    On
TraceLog "||/opt/FJSVahs/bin/ahsrlog -d /opt/FJSVahs/logs/tracelog 1 5"
```

When trace log file rotation is performed in units of file size



Example

Windows32/64

When trace log file rotation is performed according to the following conditions:

- File Size: 2 MB
- File Name: C:\Interstage\F3FMahs\logs\tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/tracelog\" 2 5"
```

Solaris32/64 **Linux32/64**

When trace log file rotation is performed according to the following conditions:

- File Size: 2 MB
- File Name: /var/opt/FJSVahs/logs/tracelog
- File count upper limit: 5

```
Trace      On
TraceLog  " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/tracelog 2 5"
```

Information

Related Directives

- [Trace](#)
- [TraceLog](#)

3.7 Setting User Authentication

User authentication checks whether the user name and password are registered in the password file when the request for access from the web browser is made. Access is denied if the user name and password are not registered in the password file.

To set user authentication, perform the following procedures:

1. [Register a User Password](#)
2. [Set User Authentication in the Environment Definition File \(httpd.conf\)](#)

(1) Register a User Password

Register a password for users to whom access permission is to be provided in the password file, by executing the [htpasswd](#) command after the command prompt.

Example

Windows32/64

Creating a password file "C:\Interstage\F3FMahs\conf\password.txt" and registering a password for user 'user1'

```
C:\Interstage\F3FMahs\bin\htpasswd.exe -c C:\Interstage\F3FMahs\conf\password.txt user1
```

Solaris32/64 **Linux32/64**

Creating a password file "/opt/FJSVahs/conf/password.txt" and registering a password for user 'user1'

```
/opt/FJSVahs/bin/htpasswd -c /opt/FJSVahs/conf/password.txt user1
```

Note

- To register subsequent users or to change a user password already registered, do not specify the `htpasswd` "-c" option.
- To delete a user, edit the password file by using a text editor.

The contents of the password file appear as follows when it is referenced using a text editor. To delete 'user2', delete the line containing 'user2' and save the file.

```
user1:$apr1$SR3.....$4aQAE2EU9NZTtbkxMEOa4/  
user2:$apr1$DS3.....$tEb4EYLhraAc1p2wIygTV/
```

- It is recommended that you change the access privileges for files created by this command:

Windows32/64

1. Start Windows Explorer.
2. Right-click the password file, then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.
4. Select "Deny" for [Full control] for all groups except SYSTEM and Administrators.

Solaris32/64 Linux32/64

1. Login as superuser.
2. Change the file access privileges to "640".

```
chmod 640 <file>
```

3. Change the file owner to "root".

```
chown root <file>
```

4. Change the file group to "nobody" (the value set for the environment definition file (`httpd.conf`) Group directive).

```
chgrp nobody <file>
```

(2) Set User Authentication in the Environment Definition File (`httpd.conf`)

Set user authentication so that only users registered in the password file are allowed to access content under the specified directory using directives such as `AuthUserFile` or `AuthType`.

Examples of allowing access to users (and hosts) are as follows:

- To allow access to only users registered in the password file
- To allow access to users registered in the password file and specified hosts

Note

When user authentication is set for the Servlet service application URL, the `<Directory>` section of the following example cannot be used. Use the `<Location>` section.

To allow access to only users registered in the password file

Example

Windows32/64

Allowing users whose names and passwords have been registered in the password file "C:\Interstage\F3FMahs\conf\password.txt" to access directories under a specified directory "C:\Interstage\F3FMahs\htdocs\users\name"

```
LoadModule auth_basic_module "C:/Interstage/F3FMahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "C:/Interstage/F3FMahs/modules/mod_authn_file.so"
LoadModule authz_user_module "C:/Interstage/F3FMahs/modules/mod_authz_user.so"
<Directory "C:/Interstage/F3FMahs\htdocs/users/name">
    AuthUserFile "C:/Interstage/F3FMahs/conf/password.txt"
    AuthName     "Secret directory"
    AuthType     Basic
    Require      valid-user
</Directory>
```

Solaris32/64 Linux32/64

Allowing users whose names and passwords have been registered in the password file "/opt/FJSVahs/conf/password.txt" to access directories under a specified directory "/opt/FJSVahs\htdocs/users/name"

```
LoadModule auth_basic_module "/opt/FJSVahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "/opt/FJSVahs/modules/mod_authn_file.so"
LoadModule authz_user_module "/opt/FJSVahs/modules/mod_authz_user.so"
<Directory "/opt/FJSVahs\htdocs/users/name">
    AuthUserFile "/opt/FJSVahs/conf/password.txt"
    AuthName     "Secret directory"
    AuthType     Basic
    Require      valid-user
</Directory>
```

To allow access to users registered in the password file and specified hosts

Example

Windows32/64

Allowing access to content under the specified directory "C:\Interstage\F3FMahs\htdocs\users\name" from either of the following:

- User to be registered in password file "C:\Interstage\F3FMahs\conf\password.txt" (User Authentication)
- Host "192.168.1.1" (IP Access Control)

```
LoadModule auth_basic_module "C:/Interstage/F3FMahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "C:/Interstage/F3FMahs/modules/mod_authn_file.so"
LoadModule authz_user_module "C:/Interstage/F3FMahs/modules/mod_authz_user.so"
<Directory "C:/Interstage/F3FMahs\htdocs/users/name">
    AuthUserFile "C:/Interstage/F3FMahs/conf/password.txt"
    AuthName     "Secret directory"
    AuthType     Basic
    Require      valid-user
    Order        Deny,Allow
    Deny         from all
    Allow        from 192.168.1.1
    Satisfy      Any
</Directory>
```

Solaris32/64 Linux32/64

Allowing access to content under the specified directory "/opt/FJSVahs\htdocs/users/name" from either of the following:

- User to be registered in password file "/opt/FJSVahs/conf/password.txt" (User Authentication)
- Host "192.168.1.1" (IP Access Control)

```
LoadModule auth_basic_module "/opt/FJSVahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "/opt/FJSVahs/modules/mod_authn_file.so"
LoadModule authz_user_module "/opt/FJSVahs/modules/mod_authz_user.so"
<Directory "/opt/FJSVahs/htdocs/users/name">
    AuthUserFile "/opt/FJSVahs/conf/password.txt"
    AuthName      "Secret directory"
    AuthType      Basic
    Require       valid-user
    Order         Deny,Allow
    Deny          from all
    Allow         from 192.168.1.1
    Satisfy       Any
</Directory>
```

Information

Related Directives

- Allow
- AuthName
- AuthType
- AuthUserFile
- Deny
- <Directory>
- LoadModule
- Order
- Require
- Satisfy

3.8 Setting IP Access Control

For IP access control, you can allow only specified hosts to make access to directories under a specified directory using the following directives in the environment definition file (httpd.conf). By doing this, any access from web browsers that are on unspecified hosts are rejected.

The following examples are shown:

- To allow a specified host to access directories under a specified directory
- To allow specified two hosts to access directories under a specified directory
- To allow a specified IPv6 address to access directories under a specified directory
- To allow a specified domain to access directories under a specified directory
- To allow only hosts configured as environment variables access to content under a specified directory

Note

When IP access control is set for the Servlet service application URL, the <Directory> section of the above example cannot be used. Use the <Location> section.

To allow a specified host to access directories under a specified directory

Example

Windows32/64

Allowing a specified host "192.168.1.1" to access directories under a specified directory "C:\Interstage\F3FMahs\htdocs\secret"

```
<Directory "C:/Interstage/F3FMahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 192.168.1.1
</Directory>
```

Solaris32/64 **Linux32/64**

Allowing a specified host "192.168.1.1" to access directories under a specified directory "/opt/FJSVahs/htdocs/secret"

```
<Directory "/opt/FJSVahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 192.168.1.1
</Directory>
```

To allow specified two hosts to access directories under a specified directory

Example

Windows32/64

Allowing specified hosts "192.168.1.1" and "192.168.1.2" to access directories under a specified directory "C:\Interstage\F3FMahs\htdocs\secret"

```
<Directory "C:/Interstage/F3FMahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 192.168.1.1 192.168.1.2
</Directory>
```

Solaris32/64 **Linux32/64**

Allowing specified hosts "192.168.1.1" and "192.168.1.2" to access directories under a specified directory "/opt/FJSVahs/htdocs/secret"

```
<Directory "/opt/FJSVahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 192.168.1.1 192.168.1.2
</Directory>
```

To allow a specified IPv6 address to access directories under a specified directory

Example

Windows32/64

Allowing a specified host "2001:db8::a00:20ff:fea7:ccea" to access directories under a specified directory "C:\Interstage\F3FMahs\htdocs\secret"

```
<Directory "C:/Interstage/F3FMahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 2001:db8::a00:20ff:fea7:ccea
</Directory>
```

Solaris32/64 Linux32/64

Allowing a specified host "2001:db8::a00:20ff:fea7:ccea" to access directories under a specified directory "/opt/FJSVahs/htdocs/secret":

```
<Directory "/opt/FJSVahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from 2001:db8::a00:20ff:fea7:ccea
</Directory>
```

To allow a specified domain to access directories under a specified directory

Example

Windows32/64

Allowing a specified domain "allow-domain.com" to access directories under a specified directory "C:\Interstage\F3FMahs\htdocs\secret"

```
<Directory "C:/Interstage/F3FMahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from allow-domain.com
</Directory>
```

Solaris32/64 Linux32/64

Allowing a specified domain "allow-domain.com" to access directories under a specified directory "/opt/FJSVahs/htdocs/secret"

```
<Directory "/opt/FJSVahs/htdocs/secret">
  Order Deny,Allow
  Deny from all
  Allow from allow-domain.com
</Directory>
```

To allow only hosts configured as environment variables access to content under a specified directory

Example

Windows32/64

Allowing hosts configured as environment variables from "192.168.1.1" to "192.168.1.9" access to content under the directory specified as "C:\Interstage\F3FMahs\htdocs\secret"

```
SetEnvIf Remote_Addr "^192\.168\.1\.[1-9]$" let_me_in
<Directory "C:/Interstage/F3FMahs/htdocs/secret">
```



```
Order Deny,Allow
Deny from all
Allow from env=let_me_in
</Directory>
```

Solaris32/64 **Linux32/64**

Allowing hosts configured as environment variables from "192.168.1.1" to "192.168.1.9" access to content under the directory specified as "/opt/FJSVahs/htdocs/secret"

```
SetEnvIf Remote_Addr "^192\.168\.1\.[1-9]$" let_me_in
<Directory "/opt/FJSVahs/htdocs/secret">
    Order Deny,Allow
    Deny from all
    Allow from env=let_me_in
</Directory>
```



Information

Related Directives

- Allow
- Deny
- <Directory>
- Order
- SetEnvIf

3.9 Setting Client Authentication

In Client Authentication (certificate authentication), an SSL environment is built and access control is performed using a client certificate sent from the client during SSL communication.

By setting authentication conditions for the client certificate attribute information in the environment definition file (httpd.conf), access control can also be performed using the client certificate condition settings.

The procedure for setting Client Authentication (certificate authentication) is shown below.

1. Build the SSL environment.

For details, refer to the "[3.10 Setting the SSL](#)".

To use certificate/key management environment SSL that was built using the SMEE command, specify "with client authentication" at the environment definition file (httpd.conf).

2. Set the environment definition file (httpd.conf).

For details on how to set the file (httpd.conf), refer below.

Set the Environment Definition File (httpd.conf)

A sample of the environment definition file (httpd.conf) is displayed below:

```
SSLCertExpand On (1)
SSLNotifyVers On (2)
RewriteEngine On (3)
```

```

RewriteCond %{ENV:EnvVarA} CondPatternA (4)
RewriteCond %{ENV:EnvVarB} CondPatternB
RewriteRule .* - [L] (5)

RewriteCond %{ENV:EnvVarC} CondPatternC
RewriteCond %{ENV:EnvVarD} CondPatternD
RewriteRule .* - [L]

RewriteRule .* - [F] (6)

```

1. **SSLCertExpand**: Enables/disables the client certificate information environment variable settings. Specify "On" for this directive. Optional (default: On).
2. **SSLNotifyVers**: Enables/disables the SSL-related environment variable settings. Specify "On" for this directive. Optional (default: On).
3. **RewriteEngine**: Enables/disables the rewrite feature. Specify "On" for this directive.
4. **RewriteCond**: Sets the authentication permissions conditions for the client certificate attribute information, and contains the condition pattern for the specified environment variable.

The environment variables that can be selected are listed below. Note that these environment variables are used to control web server behavior, not the operating system.

Environment variable	Client certificate item
SSL_CLIENT_CN	First and last name
SSL_CLIENT_C	Country
SSL_CLIENT_EMAIL	Mail address
SSL_CLIENT_O	Organization name
SSL_CLIENT_OU	Organizational unit name
SSL_CLIENT_T	Title
SSL_CLIENT_PHONE	Telephone number
SSL_CLIENT_ST	State/Prefecture
SSL_CLIENT_L	Street

For CondPattern, specify a regular expression that determines the environment variable value. To negate the pattern, prefix it with an exclamation mark (!). Strings containing spaces must be enclosed in double quotation marks (").

5. **RewriteRule**: If "[L]" is specified, this directive sets the access permissions according to the authentication permissions specified in **RewriteCond**.

Point

It is possible to specify multiple **RewriteCond** directives before the **RewriteRule** directive (with the [L] flag) to set authentication permissions conditions that will be used together.

6. **RewriteRule**: If "[F]" is specified, this directive sets the access denial to the client that sent the client certificate that did not match the authentication permissions conditions set above.

Note

When the Client Authentication (authentication using the certificate condition settings) access control is set for the Servlet service application URL, the <Directory> section of the above example cannot be used. Use the <Location> section.

An example of definition in the environment definition file (httpd.conf) for each case is shown below.

- [Authentication Condition Settings for an Organization](#)
- [Authentication Condition Settings for a Locale](#)

Authentication Condition Settings for an Organization



Example

Allowing access using a client certificate that matches one of the following conditions:

- Organization name is "organizationA", and organizational unit name is "organizationAunit1" or "organizationAunit2"
- Organization name is not "organizationB", or organizational unit name is neither "organizationBunit1" nor "organizationBunit2"
- Organization name is a string that starts with "organization" (no case sensitivity), and title is a string that contains "Manager"

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationA$
RewriteCond %{ENV:SSL_CLIENT_OU} ^organizationAunit1$|^organizationAunit2$
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationB$
RewriteCond %{ENV:SSL_CLIENT_OU} !(^organizationBunit1$|^organizationBunit2$)
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} "^organization.*" [NC]
RewriteCond %{ENV:SSL_CLIENT_T} .*Manager.*
RewriteRule .* - [L]

RewriteRule .* - [F]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationA$
RewriteCond %{ENV:SSL_CLIENT_OU} ^organizationAunit1$|^organizationAunit2$
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationB$
RewriteCond %{ENV:SSL_CLIENT_OU} !(^organizationBunit1$|^organizationBunit2$)
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} "^organization.*" [NC]
RewriteCond %{ENV:SSL_CLIENT_T} .*Manager.*
RewriteRule .* - [L]

RewriteRule .* - [F]
```

Authentication Condition Settings for a Locale

Example

Allowing access using a client certificate that matches one of the following conditions:

- Country "JP", Prefecture "Tokyo"/"Osaka"/"Kyoto"
- Country "US", State "California"/"New York"

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_C} ^JP$
RewriteCond %{ENV:SSL_CLIENT_ST} ^Tokyo$|^Osaka$|^Kyoto$
RewriteRule .* - [L,E=REMOTE_USER:JP-user]

RewriteCond %{ENV:SSL_CLIENT_C} ^US$
RewriteCond %{ENV:SSL_CLIENT_ST} "^California$|^New York$"
RewriteRule .* - [L,E=REMOTE_USER:US-user]

RewriteRule .* - [F]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_C} ^JP$
RewriteCond %{ENV:SSL_CLIENT_ST} ^Tokyo$|^Osaka$|^Kyoto$
RewriteRule .* - [L,E=REMOTE_USER:JP-user]

RewriteCond %{ENV:SSL_CLIENT_C} ^US$
RewriteCond %{ENV:SSL_CLIENT_ST} "^California$|^New York$"
RewriteRule .* - [L,E=REMOTE_USER:US-user]

RewriteRule .* - [F]
```

Information

Related Directives

- [LoadModule](#)
- [RewriteCond](#)
- [RewriteEngine](#)
- [RewriteRule](#)
- [SSLCertExpand](#)
- [SSLNotifyVers](#)

3.10 Setting the SSL

Interstage HTTP Server 2.2 can use the following two environments for managing the certificates and private keys required for encryption and signature processing.

SSL for Interstage Certificate Environments (Recommended)

To use Interstage Certificate Environment SSL communication, set the environment referring to "[3.10.1 SSL for Interstage Certificate Environments](#)".



The following function is mandatory:

- Interstage Management Console

SSL for Certificate/Key Management Environments Configured with the SMEE Commands

To use SSL communication in the certificate/key management environment that is built using the SMEE command, set the environment referring to "[3.10.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands](#)".



To use a certificate/key management environment, the following components must be installed.

- **Windows32/64**
Secure Communication Service
- **Solaris32**
FJSVisscs, FJSVsmee, FJSVslcr, and FSUNssll packages
- **Solaris64**
FJSVisscs, FJSVsmee64, and FJSVslcr64 packages
- **Linux32**
FJSVisscs, FJSVsmee and FJSVslcr packages
- **Linux64**
FJSVisscs, FJSVsmee64 and FJSVslcr64 packages

3.10.1 SSL for Interstage Certificate Environments

This section explains the environment settings required in order to use Interstage Certificate Environment SSL communication.

1. Configure the Interstage certificate environment. Refer to the "Setting and Use of the Interstage Certificate Environment" chapter of the Security System Guide.
2. Set the environment definition file (httpd.conf). Refer to the "[Configure the Environment Definition File \(httpd.conf\)](#)".

Configure the Environment Definition File (httpd.conf)

Make the SSL settings in the environment definition file (httpd.conf).

SSL can be used to perform the following operations:

- [Web server SSL definition](#)

This is an SSL definition for the entire web server. It is possible to configure SSL operations that use and do not use client authentication.

- [Virtual host SSL definition](#)

This is an SSL definition for each virtual host. Using this setting, communication that uses and does not use SSL can be operated at the same time.

Web Server SSL Definition

Example

Windows32/64

When operating SSL using the following settings:

- Port number "443"
- Server Administrator e-mail address "webmaster@main.example.com"
- Host name of Server "main.example.com"
- SSL definition name "SSL"

```
LoadModule ahs_ssl_module "C:/Interstage/F3FMahs/modules/mod_ahs_ssl.so"

Listen      443
ServerAdmin webmaster@main.example.com
ServerName  main.example.com

SSLConfName SSL
```

Solaris32/64 Linux32/64

When operating SSL using the following settings:

- Port number "443"
- Server Administrator e-mail address "webmaster@main.example.com"
- Host name of Server "main.example.com"
- User ID "user1" of user to be registered in Interstage certificate environment owner group (Note)
- Group ID "group1" of user to be registered in Interstage certificate environment owner group (Note)
- SSL definition name "SSL"

Note) This user is registered in the group created when the Interstage Certificate Environment access privileges are set. For details, refer to "Configuring Environments" - "Setting up Access Permissions in the Interstage Certificate Environment" in the "Setting and Use of the Interstage Certificate Environment" chapter of the Security System Guide.

```
LoadModule ahs_ssl_module /opt/FJSVahs/modules/mod_ahs_ssl.so

Listen      443
ServerAdmin webmaster@main.example.com
ServerName  main.example.com

User        user1
Group       group1

SSLConfName SSL
```

Virtual Host SSL Definitions

Example

Windows32/64

When operating SSL using the following settings:

- Virtual host not using SSL:
 - Port number "80"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/public"
- Virtual host using SSL
 - Port number "443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "C:\www\secure1"
 - SSL definition name "SSL1"
 - Access log file name "C:\Interstage\F3FMahs\logs\accesslog_secure1"
 - Error log file name "C:\Interstage\F3FMahs\logs\errorlog_secure1"
- Virtual host using SSL
 - Port number "8443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "C:\www\secure2"
 - SSL definition name "SSL2"
 - Access log file name "C:\Interstage\F3FMahs\logs\accesslog_secure2"
 - Error log file name "C:\Interstage\F3FMahs\logs\errorlog_secure2"

```
LoadModule ahs_ssl_module "C:/Interstage/F3FMahs/modules/mod_ahs_ssl.so"

Listen 80
Listen 443
Listen 8443

<VirtualHost 192.168.0.1:80>
    ServerName main.example.com
    DocumentRoot C:/www/public
</VirtualHost>

<VirtualHost 192.168.0.1:443>
    ServerName main.example.com
    DocumentRoot C:/www/secure1
    SSLConfName SSL1
    CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
accesslog_secure1\" 1 5" ahs-analysis
    ErrorLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
errorlog_secure1\" 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
    ServerName main.example.com
```

```

DocumentRoot C:/www/secure2
SSLConfName SSL2
CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
accesslog_secure2\" 1 5" ahs-analysis
ErrorLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
errorlog_secure2\" 1 5"
</VirtualHost>

```

Solaris32/64 Linux32/64

When operating SSL using the following settings:

- User ID "user1" of user to be registered in Interstage certificate environment owner group (Note)
- Group ID "group1" of user to be registered in Interstage certificate environment owner group (Note)
- Virtual host not using SSL:
 - Port number "80"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/public"
- Virtual host using SSL
 - Port number "443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/secure1"
 - SSL definition name "SSL1"
 - Access log file name "/opt/FJSVahs/logs/accesslog_secure1"
 - Error log file name "/opt/FJSVahs/logs/errorlog_secure1"
- Virtual host using SSL
 - Port number "8443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/secure2"
 - SSL definition name "SSL2"
 - Access log file name "/opt/FJSVahs/logs/accesslog_secure2"
 - Error log file name "/opt/FJSVahs/logs/errorlog_secure2"

Note) This user is registered in the group created when the Interstage Certificate Environment access privileges are set. For details, refer to "Configuring Environments" - "Setting up Access Permissions in the Interstage Certificate Environment" in the "Setting and Use of the Interstage Certificate Environment" chapter of the Security System Guide.

```

LoadModule ahs_ssl_module /opt/FJSVahs/modules/mod_ahs_ssl.so

Listen 80
Listen 443
Listen 8443

User user1
Group group1

<VirtualHost 192.168.0.1:80>
    ServerName main.example.com
    DocumentRoot /home/www/public
</VirtualHost>

```



```

<VirtualHost 192.168.0.1:443>
  ServerName    main.example.com
  DocumentRoot  /home/www/secure1
  SSLConfName   SSL1
  CustomLog " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog_secure1 1 5" ahs-analysis
  ErrorLog " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/errorlog_secure1 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
  ServerName    main.example.com
  DocumentRoot  /home/www/secure2
  SSLConfName   SSL2
  CustomLog " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog_secure2 1 5" ahs-analysis
  ErrorLog " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/errorlog_secure2 1 5"
</VirtualHost>

```

Note

The Site Certificate and CA Certificate both have a validity term, after which they will expire. If a web server operation continues after this validity term has expired, the error message "ahs00504"/"ahs00505" is output and it will not be possible to perform web server start/communication processing. Check the validity term of the certificate in the following Interstage Management Console windows and obtain and then register a new certificate before this validity term expires.

- [System] > [Security] > [Certificates] > [CA Certificate]
- [System] > [Security] > [Certificates] > [Site Certificate]

Note that, before the validity term of the Site Certificate and the CA Certificate expires, it is possible to specify that a warning message that notifies the number of days the certificate is still valid for ("ahs00536"/"ahs00537") be output at the required time.

An example of the environment definition file (httpd.conf) definitions is shown below.

Example: How to specify that the warning message ("ahs00536"/"ahs00537") that notifies the number of days the Site Certificate and CA Certificate are still valid for be output at the following times:

- Whenever the web server is started, in a period that starts from 15 days before the certificate expires until the expiry date
- At 9:30 10 days before the validity term of the certificate expires (while the web server is running)
- At 9:30 3 days before the validity term of the certificate expires (while the web server is running)
- At 9:30 1 day before the validity term of the certificate expires (while the web server is running)

```
SSLCertExpire All 15 10,3,1:093000
```

Information

Related Directives

- CustomLog
- DocumentRoot
- ErrorLog
- Group
- Listen
- LoadModule

- ServerAdmin
- ServerName
- [SSLCertExpire](#)
- [SSLConfName](#)
- User
- <VirtualHost>

3.10.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands

This section explains the environment settings that are required in order to use SSL communication in the certificate/key management environment that is built using the SMEE command.

1. Create a certificate/key management environment.

For details, refer to "Creating a Certificate/Key Management Environment" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter of the Security System Guide.

2. Create a secret key and acquire a certificate.

For details, refer to "Creating a Private Key and Acquiring a Certificate" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter of the Security System Guide.

3. Register the certificate and CRL.

For details, refer to "Registering the Certificate and CRL" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter of the Security System Guide.

4. Register the user PIN.

For details, refer to "[Registering the User PIN](#)"

5. Set the environment definition file.

For details, refer to "[Setting the Environment Definition file \(httpd.conf\)](#)".

6. Register CA certificate on the web browser.

For details, refer to "Operating the Client Certificate" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter of the Security System Guide.



Note

Solaris32/64 **Linux32/64**

When performing client authentication, a user other than the superuser authority needs to execute Steps 1 to 3.

In addition, specify the user or group in the environment definition file in step 5.

Registering the User PIN

Register the user PIN in the user PIN management file.

By specifying the user PIN and user PIN management file in the [ihsregistupin](#) command, the user PIN is registered in the user PIN management file after encrypting it.



Example

Windows32/64

When the user PIN (dialog input) is encrypted and registered to the user PIN management file "d:\ssl\upinfile"

```
C:\Interstage\F3FMahs\bin\ihsregistupin.exe -f d:\ssl\upinfile -d d:\sslenv\slot
```

Solaris32/64 Linux32/64

When the user PIN (dialog input) is encrypted and registered to the user PIN management file "/home/ssl/upinfile"

```
/opt/FJSVahs/bin/ihsregistupin -f /home/ssl/upinfile -d /home/sslenv/slot
```



Note

Windows32/64

We recommend changing the access privileges for the user PIN admin file:

1. Start Windows Explorer.
2. Right-click the user PIN admin file, then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.
4. Select "Deny" for [Allow Access] for all groups except SYSTEM and Administrators.

Setting the Environment Definition file (httpd.conf)

Make the SSL settings in the environment definition file (httpd.conf).

SSL can be used to perform the following operations:

- [Web server SSL definition](#)

This is an SSL definition for the entire web server. It is possible to configure SSL operations that use and do not use client authentication.

- [Virtual host SSL definitions](#)

This is an SSL definition for each virtual host. Using this setting, communication that uses and does not use SSL can be operated at the same time.

Web Server SSL Definition



Example

Windows32/64

When operating SSL using the following settings:

- Port number "443"
- Server Administrator e-mail address "webmaster@main.example.com"
- Host name of Server "main.example.com"

- SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
- Verifies a client certificate.
- Slot information directory "d:\ssl\slotdir"
- Token label "secret_key_tok"
- User PIN file "d:\ssl\upinfile"
- Operation control directory "d:\ssl\envdir"
- Nickname of the site certificate "server_cert"
- Nickname of the client CA certificate "client_cert"
- Encryption method "SSL_TXT_RSA_WITH_AES_256_CBC_SHA, SSL_TXT_RSA_WITH_AES_128_CBC_SHA, SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA"

```
LoadModule ahs_ssl_module "C:/Interstage/F3FMahs/modules/mod_ahs_ssl.so"

Listen      443
ServerAdmin webmaster@main.example.com
ServerName  main.example.com

SSLExec      On
SSLVersion   3-3.1
SSLVerifyClient require
SSLSlotDir   d:/ssl/slotdir
SSLTokenLabel secret_key_tok
SSLUserPINFile d:/ssl/upinfile
SSEnvDir     d:/ssl/envdir
SSLCertName  server_cert
SSLClCACertName client_cert
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA
```

Solaris32/64 Linux32/64

When operating SSL using the following settings:

- Port number "443"
- Server Administrator e-mail address "webmaster@main.example.com"
- Host name of Server "main.example.com"
- User of creating a certificate/key management environment "user1"
- Group of creating a certificate/key management environment "group1"
- SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
- Verifies a client certificate.
- Slot information directory "/home/ssl/slotdir"
- Token label "secret_key_tok"
- User PIN file "/home/ssl/upinfile"
- Operation control directory "/home/ssl/envdir"
- Nickname of the site certificate "server_cert"
- Nickname of the client CA certificate "client_cert"
- Encryption method "SSL_TXT_RSA_WITH_AES_256_CBC_SHA, SSL_TXT_RSA_WITH_AES_128_CBC_SHA, SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA"

```
LoadModule ahs_ssl_module /opt/FJJSVahs/modules/mod_ahs_ssl.so

Listen      443
ServerAdmin webmaster@main.example.com
ServerName  main.example.com

User  user1
Group group1

SSLExec      On
SSLVersion   3-3.1
SSLVerifyClient require
SSLSlotDir   /home/ssl/slotdir
SSLTokenLabel secret_key_tok
SSLUserPINFile /home/ssl/upinfile
SSLEnvDir    /home/ssl/envdir
SSLCertName  server_cert
SSLClCACertName client_cert
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA
```

Virtual Host SSL Definitions



Example

Windows32/64

When operating SSL using the following settings:

- Slot information directory "d:\ssl\slotdir"
- Token label "secret_key_tok"
- User PIN file "/d:\ssl\upinfile"
- Virtual host not using SSL:
 - Port number "80"
 - Host name of Server "main.example.com"
 - Operation control directory "C:\www\public"
- Virtual host using SSL (without client authentication):
 - Port number "443"
 - Host name of Server "main.example.com"
 - Operation control directory "C:\www\secure1"
 - SSL protocol version "SSL2.0"
 - Operation control directory "d:\ssl\envdir"
 - Nickname of the site certificate "cert_for_purchase"
 - Access log file name "/C:\Interstage\F3FMahs\logs\accesslog_secure1"
 - Error log file name "C:\Interstage\F3FMahs\logs\errorlog_secure1"
- Virtual host using SSL (with client authentication):
 - Port number "8443"
 - Host name of Server "main.example.com"

- Operation control directory "C:\www\secure2"
- SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
- Operation control directory "d:\ssl\envdir"
- Nickname of the site certificate "cert_for_manager"
- Nickname of the client CA certificate "CACert_InfoCA"
- Encryption method "SSL_TXT_RSA_WITH_AES_256_CBC_SHA, SSL_TXT_RSA_WITH_AES_128_CBC_SHA, SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA"
- Access log file name "/C:\Interstage\F3FMahs\logs\accesslog_secure2"
- Error log file name "C:\Interstage\F3FMahs\logs\errorlog_secure2"

```

LoadModule ahs_ssl_module "C:/Interstage/F3FMahs/modules/mod_ahs_ssl.so"

Listen 80
Listen 443
Listen 8443

SSLSlotDir      d:/ssl/slotdir
SSLTokenLabel   secret_key_tok
SSLUserPINFile  d:/ssl/upinfile

<VirtualHost 192.168.0.1:80>
    ServerName    main.example.com
    DocumentRoot  C:/www/public
</VirtualHost>

<VirtualHost 192.168.0.1:443>
    ServerName    main.example.com
    DocumentRoot  C:/www/secure1
    SSLExec       On
    SSLVersion    2
    SSLEnvDir     d:/ssl/envdir
    SSLCertName   cert_for_purchase
    CustomLog     "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
accesslog_secure1\" 1 5" ahs-analysis
    ErrorLog      "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
errorlog_secure1\" 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
    ServerName    main.example.com
    DocumentRoot  C:/www/secure2
    SSLExec       On
    SSLVersion    3-3.1
    SSLVerifyClient require
    SSLEnvDir     d:/ssl/envdir
    SSLCertName   cert_for_manager
    SSLC1CACertName CACert_InfoCA
    SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA
    CustomLog     "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
accesslog_secure2\" 1 5" ahs-analysis
    ErrorLog      "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/
errorlog_secure2\" 1 5"
</VirtualHost>

```

Solaris32/64 Linux32/64

When operating SSL using the following settings:

- User of creating a certificate/key management environment "user1"
- Group of creating a certificate/key management environment "group1"
- Slot information directory "/home/ssl/slotdir"
- Token label "secret_key_tok"
- User PIN file "/home/ssl/upinfile"
- Virtual host not using SSL:
 - Port number "80"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/public"
- Virtual host using SSL (without client authentication):
 - Port number "443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/secure1"
 - SSL protocol version "SSL2.0"
 - Operation control directory "/home/ssl/envdir"
 - Nickname of the site certificate "cert_for_purchase"
 - Access log file name "//opt/FJSVahs/logs/accesslog_secure1"
 - Error log file name "/opt/FJSVahs/logs/errorlog_secure1"
- Virtual host using SSL (with client authentication):
 - Port number "8443"
 - Host name of Server "main.example.com"
 - Root directory open to the public "/home/www/secure2"
 - SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
 - Operation control directory "/home/ssl/envdir"
 - Nickname of the site certificate "cert_for_manager"
 - Nickname of the client CA certificate "CACert_InfoCA"
 - Encryption method "SSL_TXT_RSA_WITH_AES_256_CBC_SHA, SSL_TXT_RSA_WITH_AES_128_CBC_SHA, SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA"
 - Access log file name "//opt/FJSVahs/logs/accesslog_secure2"
 - Error log file name "/opt/FJSVahs/logs/errorlog_secure2"

```

LoadModule ahs_ssl_module /opt/FJSVahs/modules/mod_ahs_ssl.so

Listen 80
Listen 443
Listen 8443

User user1
Group group1

SSLSlotDir      /home/ssl/slotdir
SSLTokenLabel   secret_key_tok
SSLUserPINFile  /home/ssl/upinfile

```

```

<VirtualHost 192.168.0.1:80>
    ServerName    main.example.com
    DocumentRoot  /home/www/public
</VirtualHost>

<VirtualHost 192.168.0.1:443>
    ServerName    main.example.com
    DocumentRoot  /home/www/secure1
    SSLExec       On
    SSLVersion    2
    SSLEnvDir     /home/ssl/envdir
    SSLCertName   cert_for_purchase
    CustomLog     "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog_secure1 1 5" ahs-analysis
    ErrorLog      "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/errorlog_secure1 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
    ServerName    main.example.com
    DocumentRoot  /home/www/secure2
    SSLExec       On
    SSLVersion    3-3.1
    SSLVerifyClient require
    SSLEnvDir     /home/ssl/envdir
    SSLCertName   cert_for_manager
    SSLCACertName CACert_InfoCA
    SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA
    CustomLog     "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog_secure2 1 5" ahs-analysis
    ErrorLog      "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/errorlog_secure2 1 5"
</VirtualHost>

```



Note

The Site Certificate and CA Certificate both have a validity term, after which they will expire. If a web server operation continues after this validity term has expired, the error message "ahs00504"/"ahs00505" is output and it is not possible to perform web server start/communication processing. Check the validity term of the certificate using the `cmdspcert` command, and obtain and then register a new certificate before this validity term expires.

Note that, before the validity term of the Site Certificate and the CA Certificate expires, it is possible to specify that a warning message that notifies the number of days the certificate is still valid for ("ahs00536"/"ahs00537") be output at the required time.

An example of the environment definition file (`httpd.conf`) definitions is shown below.

Example: How to specify that the warning message ("ahs00536"/"ahs00537") that notifies the number of days the Site Certificate and CA Certificate are still valid for be output at the following times:

- Whenever the web server is started, in a period that starts from 15 days before the certificate expires until the expiry date
- At 9:30 10 days before the validity term of the certificate expires (while the web server is running)
- At 9:30 3 days before the validity term of the certificate expires (while the web server is running)
- At 9:30 1 day before the validity term of the certificate expires (while the web server is running)

```
SSLCertExpire All 15 10,3,1:093000
```



Information

Related Directives

- CustomLog
- DocumentRoot
- ErrorLog
- Group
- Listen
- LoadModule
- ServerAdmin
- ServerName
- SSLCertExpire
- SSLConfName
- SSLCICACertName
- SSLCipherSuite
- SSLEnvDir
- SSLExec
- SSLSlotDir
- SSLTokenLabel
- SSLUserPINFile
- SSLVerifyClient
- SSLVersion
- User
- <VirtualHost>



3.11 Setting the Virtual Host

The IP/port number-based virtual host or name-based virtual host is set using the <VirtualHost> section or NameVirtualHost directive. Using this setting, multiple virtual machines can be used from the web browser.

The following examples are shown:

- IP-based virtual hosts
- Port number-based virtual hosts
- IP and port number-based virtual hosts
- Name-based virtual hosts

IP-based virtual hosts



Example

Setting the main host "main.example.com" as IP address "192.168.0.1", and the virtual host "virt.example.com" as IP address "192.168.0.2"

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...
```

```
<VirtualHost 192.168.0.2>
  ServerName virt.example.com
  ServerAdmin webmaster@virt.example.com
  ...
</VirtualHost>
```

Setting the virtual host "virt.example.com" as IPv6 address "2001:db8::a00:20ff:fea7:ccea"

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...
<VirtualHost [2001:db8::a00:20ff:fea7:ccea]>
  ServerName virt.example.com
  ServerAdmin webmaster@virt.example.com
  ...
</VirtualHost>
```

Port number-based virtual hosts



Example

Setting the virtual host "virt1.example.com" to use port number "8000", and the virtual host "virt2.example.com" to use port number "9000"

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...

Listen 8000
Listen 9000

<VirtualHost _default_:8000>
  ServerName virt1.example.com
  ServerAdmin webmaster@virt1.example.com
  ...
</VirtualHost>

<VirtualHost _default_:9000>
  ServerName virt2.example.com
  ServerAdmin webmaster@virt2.example.com
  ...
</VirtualHost>
```

IP and port number-based virtual hosts



Example

Setting the virtual host "virt1.example.com" as IP address "192.168.0.2" using port number "8000", and virtual host "virt2.example.com" as IP address "192.168.0.3" using port number "9000"

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...

Listen 192.168.0.2:8000
Listen 192.168.0.3:9000
```

```

...
<VirtualHost 192.168.0.2:8000>
    ServerName    virt1.example.com
    ServerAdmin   webmaster@virt1.example.com
    ...
</VirtualHost>

<VirtualHost 192.168.0.3:9000>
    ServerName    virt2.example.com
    ServerAdmin   webmaster@virt2.example.com
    ...
</VirtualHost>

```

Setting the virtual host "virt1.example.com" as IPv6 address "2001:db8::a00:20ff:fea7:ccea" using port number "8000", and virtual host "virt2.example.com" as IPv6 address "2001:db8::a00:20ff:fea7:cceb" using port number "9000"

```

ServerAdmin   webmaster@main.example.com
ServerName    main.example.com
...

Listen 8000
Listen 9000
...
<VirtualHost [2001:db8::a00:20ff:fea7:ccea]:8000>
    ServerName    virt1.example.com
    ServerAdmin   webmaster@virt1.example.com
    ...
</VirtualHost>

<VirtualHost [2001:db8::a00:20ff:fea7:cceb]:9000>
    ServerName    virt2.example.com
    ServerAdmin   webmaster@virt2.example.com
    ...
</VirtualHost>

```

Name-based virtual hosts



- SSL cannot be used.
- Set the same value in the <VirtualHost> section and the NameVirtualHost directive.
- The ServerName directive must be set.
- Requests from the client are distributed according to the ServerName directive specified in the <VirtualHost> section.
If a request is not distributed according to the ServerName directive (for example, when the IP address has been specified), the first virtual host of the name-based virtual hosts set in the environment definition file (httpd.conf) will receive the request.
- If a request from the client is received using the "IP address[:port number]" specified in the NameVirtualHost directive, the request is received using the virtual host of that "IP address[:port number]", not the main host.
To receive requests using the ServerName or DocumentRoot directive settings, for example, of the main host, add them as virtual hosts. Create the <VirtualHost> section, and then set the ServerName or DocumentRoot directives, for example, of the main host.

Example

Setting name-based virtual hosts "virt1.example.com" and "virt2.example.com"

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...

Listen 192.168.0.1:8000
NameVirtualHost 192.168.0.1:8000

<VirtualHost 192.168.0.1:8000>
    ServerName    virt1.example.com
    ServerAdmin   webmaster@virt1.example.com
    ...
</VirtualHost>

<VirtualHost 192.168.0.1:8000>
    ServerName    virt2.example.com
    ServerAdmin   webmaster@virt2.example.com
    ...
</VirtualHost>
```

Setting name-based virtual hosts "virt1.example.com" and "virt2.example.com" (when an IPv6 address is used)

```
ServerAdmin webmaster@main.example.com
ServerName main.example.com
...

Listen 8000
NameVirtualHost [2001:db8::a00:20ff:fea7:ccea]:8000

<VirtualHost [2001:db8::a00:20ff:fea7:ccea]:8000>
    ServerName    virt1.example.com
    ServerAdmin   webmaster@virt1.example.com
    ...
</VirtualHost>

<VirtualHost [2001:db8::a00:20ff:fea7:ccea]:8000>
    ServerName    virt2.example.com
    ServerAdmin   webmaster@virt2.example.com
    ...
</VirtualHost>
```

Information

Related Directives

- Listen
- NameVirtualHost
- ServerAdmin
- ServerName
- <VirtualHost>

3.12 Setting the Virtual Directory

The specified directory is set as the virtual directory using the Alias directive.

Example

Windows32/64

Setting directory "C:\Interstage\F3FMahs\htdocs\mydirectory\issue\news" as virtual directory "news"

```
Alias /news C:/Interstage/F3FMahs/htdocs/mydirectory/issue/news
```

Setting directory "C:\Interstage\F3FMahs\htdocs\mydirectory\issue\news" in the path that starts with virtual directory "news"

```
AliasMatch ^/news(.*) C:/Interstage/F3FMahs/htdocs/mydirectory/issue/news$1
```

Solaris32/64 **Linux32/64**

Setting directory "/opt/FJSVahs/htdocs/mydirectory/issue/news" as virtual directory "news"

```
Alias /news /opt/FJSVahs/htdocs/mydirectory/issue/news
```

Setting directory "/opt/FJSVahs/htdocs/mydirectory/issue/news" in the path that starts with virtual directory "news"

```
AliasMatch ^/news(.*) /opt/FJSVahs/htdocs/mydirectory/issue/news$1
```

Information

Related Directives

- Alias
 - AliasMatch
-

3.13 Setting the Redirect Function

URL redirection is set using the Redirect directive or RedirectMatch directive.

Note

To set redirect for a Servlet service application URL, set the Redirect directive or RedirectMatch directive in the <Location> section.

Example

Redirecting "/info" to "www.company.com/info"

```
Redirect seeother /info http://www.company.com/info
```

When using SSL, "https" that performs SSL communication can also be specified in the URL path.

```
Redirect seeother /info https://www.company.com/info
```

Redirecting a GIF file to a JPEG file of the same name on another server (www.company.com)

```
RedirectMatch (.*)\.gif$ http://www.company.com$1.jpg
```

Information

Related Directives

- Redirect
- RedirectMatch

3.14 Setting the Rewrite Function

The rewrite function sets the URL rewrite conditions and rules as a regular expression using the Rewrite-related directive. Through this setting, the URL is rewritten when the rewrite conditions and rules are satisfied.

The following examples are shown:

- [Rewriting a URL using a client IP address](#)
- [Rewriting a URL using a request URL negation condition](#)
- [Blocking access according to the request method type](#)
- [Displaying different pages according to the browser type](#)
- [Redirecting Servlet service application URLs](#)
- [Forcing the rewritten URL to be a proxy request](#)
- [Executing CGI from the rewritten URL](#)

Note

- In the virtual host, set the rewrite function directive for each virtual host.
- To set the rewrite function for a Servlet service application URL, set the rewrite function directive in the <Location> section.
- If the rewritten URL is a Servlet service application URL, only external redirection is valid.

Rewriting a URL using a client IP address

Example

Redirecting the URL to "/ext" internally when the client IP address starts with "192.168.0"

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond %{REMOTE_ADDR} ^192\.168\.0\.
RewriteRule ^/(.*)$ /ext/$1
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond  %{REMOTE_ADDR} ^192\.168\.0\.
RewriteRule  ^/(.*)$ /ext/$1
```

Rewriting a URL using a request URL negation condition

Example

Redirecting a URL to "otherhost" externally when the first part of the URL string from the web browser (client) is not "/somepath"

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond  %{REQUEST_URI} !~/somepath
RewriteRule  ^/(.*)$ http://otherhost/$1
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond  %{REQUEST_URI} !~/somepath
RewriteRule  ^/(.*)$ http://otherhost/$1
```

Blocking access according to the request method type

Example

Responding using status code "403" (Forbidden) if a HEAD method or OPTIONS method request was received

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond  %{REQUEST_METHOD} ^(HEAD|OPTIONS)$
RewriteRule  .* - [F]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
```

```
RewriteCond    %{REQUEST_METHOD} ^(HEAD|OPTIONS)$
RewriteRule    .* - [F]
```

Displaying different pages according to the browser type

Example

Displaying different pages according to the accessed web browser type

- Internet Explorer: html pages with "-i" appended to the file name
- Non-Internet Explorer browsers: html pages with "-o" appended to the file name

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond    %{HTTP_USER_AGENT} .*MSIE.*
RewriteRule    ^/(.*)\.html /$1-i.html [L]
RewriteRule    ^/(.*)\.html /$1-o.html [L]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond    %{HTTP_USER_AGENT} .*MSIE.*
RewriteRule    ^/(.*)\.html /$1-i.html [L]
RewriteRule    ^/(.*)\.html /$1-o.html [L]
```

Redirecting Servlet service application URLs

Example

Redirecting the URL to "sample2" externally, when the URL in the web browser (client) contains the Servlet service application identifier "sample1"

Note) All parts of the URL except "/sample1/" specified in the <Location> section are evaluated using the RewriteRule directive.

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

<Location /sample1/>
  RewriteEngine On
  RewriteRule    ^(.*)$ /sample2/$1 [R]
</Location>
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

<Location /sample1/>
```



```
RewriteEngine On
RewriteRule ^(.*)$ /sample2/$1 [R]
</Location>
```

Forcing the rewritten URL to be a proxy request



Example

Treating a URL in which "/info/" is specified at the start of the string from the web browser (client) as a proxy request, and forwarding the request to "originhost"

Note) If the URL is "/info", the proxy action is executed after the URL is rewritten to "/info/". "https" cannot be specified as the forwarded request.

Windows32/64

```
LoadModule rewrite_module      "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
LoadModule proxy_module        "C:/Interstage/F3FMahs/modules/mod_proxy.so"
LoadModule proxy_http_module   "C:/Interstage/F3FMahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteRule ^/info$ /info/
RewriteRule ^/info/(.*)$ http://originhost/info/$1 [P]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module      "/opt/FJSVahs/modules/mod_rewrite.so"
LoadModule proxy_module        "/opt/FJSVahs/modules/mod_proxy.so"
LoadModule proxy_http_module   "/opt/FJSVahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteRule ^/info$ /info/
RewriteRule ^/info/(.*)$ http://originhost/info/$1 [P]
```

Executing CGI from the rewritten URL



Example

Executing CGI under /cgi-bin when the URL in the web browser (client) has file name extension "cgi"

Windows32/64

```
LoadModule cgi_module         "C:/Interstage/F3FMahs/modules/mod_cgi.so"
LoadModule rewrite_module     "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

ScriptAlias /cgi-bin/ "C:/Interstage/F3FMahs/cgi-bin/"
RewriteEngine On
RewriteRule ^/(.+\.cgi)$ /cgi-bin/$1 [PT]
```

Solaris32/64 Linux32/64

```
LoadModule cgid_module        "/opt/FJSVahs/modules/mod_cgid.so"
LoadModule rewrite_module     "/opt/FJSVahs/modules/mod_rewrite.so"
```

```
ScriptAlias /cgi-bin/ "/opt/FJShahs/cgi-bin/"
RewriteEngine On
RewriteRule ^/(.+\.cgi)$ /cgi-bin/$1 [PT]
```

Information

Related Directives

- LoadModule
- <Location>
- [RewriteCond](#)
- [RewriteEngine](#)
- [RewriteRule](#)
- ScriptAlias

3.15 Setting the Server Status Monitoring

Server status monitoring is set using directives such as ExtendedStatus.

Note

- This setting applies to the entire web server. It cannot be modified per virtual host.
- There is a threat that a malicious user (or machine) on the network will intercept and look at the server status information, therefore it is recommended that user authentication and IP access control be set together.

Example

Specifying the URL "http://192.168.1.1(web server IP address)/server-status" in the web browser (client), and displaying the server status information

Windows32/64

```
LoadModule auth_basic_module "C:/Interstage/F3FMahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "C:/Interstage/F3FMahs/modules/mod_authn_file.so"
LoadModule authz_user_module "C:/Interstage/F3FMahs/modules/mod_authz_user.so"
LoadModule status_module "C:/Interstage/F3FMahs/modules/mod_status.so"
ExtendedStatus On
<Location /server-status>
    AuthUserFile "C:/Interstage/F3FMahs/conf/password.txt"
    AuthName "Server Status"
    AuthType Basic
    Require valid-user
    SetHandler server-status
    Order Deny,Allow
    Deny from all
    Allow from 192.168.1.1
</Location>
```

Solaris32/64 Linux32/64

```
LoadModule auth_basic_module "/opt/FJSVahs/modules/mod_auth_basic.so"
LoadModule authn_file_module "/opt/FJSVahs/modules/mod_authn_file.so"
LoadModule authz_user_module "/opt/FJSVahs/modules/mod_authz_user.so"
LoadModule status_module     "/opt/FJSVahs/modules/mod_status.so"
ExtendedStatus On
<Location /server-status>
    AuthUserFile "/opt/FJSVahs/conf/password.txt"
    AuthName     "Server Status"
    AuthType     Basic
    Require      valid-user
    SetHandler   server-status
    Order        Deny,Allow
    Deny         from all
    Allow        from 192.168.1.1
</Location>
```

Information

Related Directives

- Allow
- AuthName
- AuthType
- AuthUserFile
- Deny
- ExtendedStatus
- <Location>
- LoadModule
- Order
- Require
- SetHandler

3.16 Setting the Compressing Content Function

Compression target content is specified and set using directives such as `SetEnvIfNoCase` or `SetOutputFilter`. Through this setting, the specified content is compressed for requests from the web browser.

The following examples are shown:

- [Compressing content other than images](#)
- [Compressing content of the MIME type "text/html"/"text/plain"](#)
- [Compressing URL content that starts with "/sample"](#)

Compressing content other than images

Example

Windows32/64

```
LoadModule headers_module "C:/Interstage/F3FMahs/modules/mod_headers.so"
LoadModule deflate_module "C:/Interstage/F3FMahs/modules/mod_deflate.so"
```

```
SetOutputFilter DEFLATE
SetEnvIfNoCase Request_URI .(?:gif|jpe?g|png)$ no-gzip dont-vary
Header append Vary User-Agent env=!dont-vary
```

Solaris32/64 **Linux32/64**

```
LoadModule headers_module "/opt/FJSVahs/modules/mod_headers.so"
LoadModule deflate_module "/opt/FJSVahs/modules/mod_deflate.so"

SetOutputFilter DEFLATE
SetEnvIfNoCase Request_URI .(?:gif|jpe?g|png)$ no-gzip dont-vary
Header append Vary User-Agent env=!dont-vary
```

Compressing content of the MIME type "text/html"/"text/plain"

Example

Windows32/64

```
LoadModule deflate_module "C:/Interstage/F3FMahs/modules/mod_deflate.so"

AddOutputFilterByType DEFLATE text/html text/plain
```

Solaris32/64 **Linux32/64**

```
LoadModule deflate_module "/opt/FJSVahs/modules/mod_deflate.so"

AddOutputFilterByType DEFLATE text/html text/plain
```

Compressing URL content that starts with "/sample"

Example

Windows32/64

```
LoadModule deflate_module "C:/Interstage/F3FMahs/modules/mod_deflate.so"

<Location /sample>
    SetOutputFilter DEFLATE
</Location>
```

Solaris32/64 **Linux32/64**

```
LoadModule deflate_module "/opt/FJSVahs/modules/mod_deflate.so"

<Location /sample>
    SetOutputFilter DEFLATE
</Location>
```

Information

Related Directives

- AddOutputFilterByType
- Header
- LoadModule
- <Location>
- SetEnvIfNoCase
- SetOutputFilter

3.17 Setting the Proxy Function

The forward proxy and reverse proxy are set using directives such as ProxyRequests or ProxyPass.

- [Forward proxy](#)
- [Reverse proxy](#)

Forward proxy

Example

Windows32/64

Building the proxy server using the following settings:

- "C:\Interstage\F3FMahs\proxy" (the directory that stores the cache file)
- "86400 minutes" (24 hours) (the expiry of the HTTP document)

```
LoadModule proxy_module          "C:/Interstage/F3FMahs/modules/mod_proxy.so"
LoadModule proxy_connect_module  "C:/Interstage/F3FMahs/modules/mod_proxy_connect.so"
LoadModule proxy_http_module     "C:/Interstage/F3FMahs/modules/mod_proxy_http.so"
LoadModule cache_module          "C:/Interstage/F3FMahs/modules/mod_cache.so"
LoadModule disk_cache_module     "C:/Interstage/F3FMahs/modules/mod_disk_cache.so"
<IfModule mod_proxy.c>
    ProxyRequests On
    CacheEnable disk /
    CacheRoot "C:/Interstage/F3FMahs/proxy"
    CacheMaxExpire 86400
</IfModule>
```

Solaris32/64 Linux32/64

Building the proxy server using the following settings:

- "/opt/FJSVahs/proxy" (the directory that stores the cache file)
- "86400 minutes" (24 hours) (the expiry of the HTTP document)

```
LoadModule proxy_module          "/opt/FJSVahs/modules/mod_proxy.so"
LoadModule proxy_connect_module  "/opt/FJSVahs/modules/mod_proxy_connect.so"
LoadModule proxy_http_module     "/opt/FJSVahs/modules/mod_proxy_http.so"
LoadModule cache_module          "/opt/FJSVahs/modules/mod_cache.so"
LoadModule disk_cache_module     "/opt/FJSVahs/modules/mod_disk_cache.so"
<IfModule mod_proxy.c>
    ProxyRequests On
```

```
CacheEnable    disk /
CacheRoot      "/opt/FJSVahs/proxy"
CacheMaxExpire 86400
</IfModule>
```

Note

Solaris32/64 **Linux32/64**

For the directory that stores the cache file, write privileges must be granted for the users configured in the User directive and the groups configured in the Group directive.

Reverse proxy

Example

Returning content under the remote server URL "http://www.company.com/info" when the URL in the web browser (client) is under "/info"

Windows32/64

```
LoadModule proxy_module          "C:/Interstage/F3FMahs/modules/mod_proxy.so"
LoadModule proxy_http_module     "C:/Interstage/F3FMahs/modules/mod_proxy_http.so"

ProxyPass      /info http://www.company.com/info
ProxyPassReverse /info http://www.company.com/info
```

Solaris32/64 **Linux32/64**

```
LoadModule proxy_module          "/opt/FJSVahs/modules/mod_proxy.so"
LoadModule proxy_http_module     "/opt/FJSVahs/modules/mod_proxy_http.so"

ProxyPass      /info http://www.company.com/info
ProxyPassReverse /info http://www.company.com/info
```

Note

When the web server that stores the content and the reverse proxy server run on one web server, two communication threads are used for one request. For this reason, the value "(normal settings value) * 2" must be configured for the number of concurrent client connections.

Information

Related Directives

- CacheEnable
- CacheMaxExpire
- CacheRoot
- <IfModule>
- LoadModule
- ProxyPass

- ProxyPassReverse
- ProxyRequests

3.18 Setting the Directory List

The directory list is set using the DirectoryIndex directive or Options directive.

Example

Displaying the directory list when the "index.html" and "index.htm" files specified in the DirectoryIndex directive do not exist

```
DirectoryIndex index.html index.htm
Options        Indexes
```

Information

Related Directives

- DirectoryIndex
- Options

3.19 Setting the Default MIME Type

The default MIME type is set using the DefaultType directive.

Example

Setting the default MIME type to "plain text" for files served with an indeterminate MIME type

```
DefaultType text/plain
```

Information

Related Directives

- DefaultType

3.20 Setting MIME Types

MIME types are set (or overridden) using the AddType directive.

Example

Serving files with a ".text" extension as "plain text"

```
AddType text/plain text
```

Information

Related Directives

- AddType

3.21 Setting the Default HTML File

The default page (HTML file, etc.) of a directory, served when the client requests an index of the directory by specifying a forward slash "/" at the end of the directory name is set using the `DirectoryIndex` directive.

Example

Setting "welcome.html" as the directory index

```
DirectoryIndex welcome.html
```

Information

Related Directives

- DirectoryIndex

3.22 Setting the HTTP Keep-Alive Function

The HTTP Keep-Alive function is set using directives such as `KeepAlive` or `KeepAliveTimeout`.

Example

Enabling the HTTP Keep-Alive function, and setting the timeout to 15 seconds and maximum number of requests to "unlimited"

```
KeepAlive On
KeepAliveTimeout 15
MaxKeepAliveRequests 0
```

Note

Even if the HTTP Keep-Alive function has been enabled, if any of the conditions below apply, it will be disabled.

- When one of the following status codes is returned to the client:
 - 400 "Bad Request"
 - 408 "Request Time-out"
 - 411 "Length Required"
 - 413 "Request Entity Too Large"
 - 414 "Request-URI Too Large"
 - 500 "Internal Server Error"
 - 501 "Not Implemented"
 - 503 "Service Temporarily Unavailable"

- A value of "1" or more is specified for the number of requests set in the MaxKeepAliveRequests directive, and "number of requests + 1" request processing has completed in the same TCP connection
- "Connection: close" is specified in the Connection header field of the HTTP request header
- "Connection: Keep-Alive" is not specified in the Connection header field of the HTTP request header (when the HTTP version is "HTTP/1.0")
- The TCP connection from the client is broken



See

The HTTP Keep-Alive function connection retention time can be checked from the trace log. For details on the HTTP Keep-Alive function connection retention time, refer to "Reference" in "4.2.3 Trace Log" - "Event Details-information"



Information

Related Directives

- KeepAlive
- KeepAliveTimeout
- MaxKeepAliveRequests

3.23 Setting User tracking Function

User tracking is set using directives such as CookieTracking or CookieExpires.



Example

Performing user tracking using a cookie that expires in three years

Windows32/64

```
LoadModule usertrack_module "C:/Interstage/F3FMahs/modules/mod_usertrack.so"
LogFormat "%{Cookie}n %r %t" cookie
CookieTracking On
CookieExpires "3 years"
CustomLog logs/usertrack.log cookie
```

Solaris32/64 Linux32/64

```
LoadModule usertrack_module "/opt/FJSVahs/modules/mod_usertrack.so"
LogFormat "%{Cookie}n %r %t" cookie
CookieTracking On
CookieExpires "3 years"
CustomLog logs/usertrack.log cookie
```



Information

Related Directives

- CookieExpires

- CookieTracking
- CustomLog
- LoadModule
- LogFormat

3.24 Setting the Cookie Log

Using the CustomLog directive, set the values for the Cookie header set in the request and the Set-Cookie header set when the response is made so that they are written to the log file.

Point

- %{Cookie}i is written in the format "NAME=value".
- %{Set-Cookie}o is written in the format "NAME=value;Expires=value;Domain=value;Path=value;secure". Note that Expires, Domain, Path, secure may be omitted by the application that is set.

Example

Writing the Cookie header and Set-Cookie header to the log file

Windows32/64

```
LoadModule log_config_module "C:/Interstage/F3FMahs/modules/mod_log_config.so"
LogFormat "%{Cookie}i %{Set-Cookie}o %r %t" cookie
CustomLog logs/cookie.log cookie
```

Solaris32/64 Linux32/64

```
LoadModule log_config_module "/opt/FJSVahs/modules/mod_log_config.so"
LogFormat "%{Cookie}i %{Set-Cookie}o %r %t" cookie
CustomLog logs/cookie.log cookie
```

Information

Related Directives

- CustomLog
- LoadModule
- LogFormat

3.25 Setting the Privileges for the Communication Process Solaris32/64

Linux32/64

The privileges for the communication process are set using the Group directive or User directive.

Note

- If the execution privileges for the communication process are changed when the Servlet service is used, the user that belongs to the web server connector log output directory must be changed to the user specified in the User directive of the web server environment definition file (httpd.conf) and granted write permission for the log output directory before the web server is started. If there are no write permissions for the log output directory, the generations of the web server connector log file cannot be managed. Check the web server connector log output directory using the wscadmin command list-web-servers subcommand. The initial value of the log output directory is "/opt/FJSVwsc/logs/jk2/(web server name)".
- When the web server connector fault monitoring function is used, and "enhanced security mode" is selected as the security setting during the installation or the privilege settings are configured in "enhanced security mode" using the issetsecuritymode command, the file and directory group shown below must be changed to the group specified in the Group directive. If the group is not changed, the web server connector fault monitoring function will not work. Note that, to use the web server connector fault monitoring function on multiple web servers, specify the same group name in the Group directive of each web server.

```
/var/opt/FJSVsvmon/.svmonsock (Note)
/var/opt/FJSVsvmon/log/svmon_api.log* (Note)
/var/opt/FJSVsvmon
/var/opt/FJSVsvmon/log
```

Note) This file is not created during installation. When the system reboots immediately after installation, a file will automatically be created in the group set in the Group directive, so there is no need to change the setting manually.

Example

Setting "apache" for the user and group as the execution privileges for the communication process

```
User apache
Group apache
```

Information

Related Directives

- Group
- User

3.26 Setting Language-based Content Negotiation

Language-based content negotiation is set using directives such as Options or AddLanguage.

Example

Windows32/64

Enabling the MultiViews function for the "C:\Interstage\F3FMahs\htdocs" directory and mapping the extensions ".ja" and ".de" to Japanese and German respectively

```
<Directory "C:/Interstage/F3FMahs/htdocs">
  Options MultiViews
</Directory>
<IfModule mod_mime.c>
  AddLanguage ja .ja
  AddLanguage de .de
</IfModule>
```

Solaris32/64 **Linux32/64**

Enabling the MultiViews function for the "/opt/FJSVahs/htdocs" directory and mapping the extensions ".ja" and ".de" to Japanese and German respectively

```
<Directory "/opt/FJSVahs/htdocs">
  Options MultiViews
</Directory>
<IfModule mod_mime.c>
  AddLanguage ja .ja
  AddLanguage de .de
</IfModule>
```

Information

Related Directives

- AddLanguage
- <Directory>
- <IfModule>
- Options

3.27 Customizing the Messages

The messages output to the access log file are customized using the LogFormat directive or CustomLog directive.

Point

Using the LogFormat directive, a customized log format is defined, and a nickname for that format is set.

Next, using the CustomLog directive, the nickname set in the ahsrlog executable statement and the LogFormat directive is specified, and the access log file format is set.

Example

Recording the client tracking information and web browser information used by the client in the access log

Windows32/64

```
LoadModule log_config_module "C:/Interstage/F3FMahs/modules/mod_log_config.so"
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
CustomLog "||\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \"C:/Interstage/F3FMahs/logs/accesslog\" 1
5" combined
```

Solaris32/64 **Linux32/64**

```
LoadModule log_config_module "/opt/FJSVahs/modules/mod_log_config.so"
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
CustomLog "/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" combined
```

Example

The following example shows the kind of information that is output for year "yyyy".

```
192.168.0.1 -- [31/Mar/yyyy:15:32:05 +0900] "GET / HTTP/1.1" 200 573 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
192.168.0.1 -- [31/Mar/yyyy:15:32:05 +0900] "GET /interstage.jpg HTTP/1.1" 200 76203 "http://ihs.fujitsu.com/" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
192.168.0.1 -- [31/Mar/yyyy:15:32:05 +0900] "GET /istage_j.gif HTTP/1.1" 200 17972 "http://ihs.fujitsu.com/" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
192.168.0.1 -- [31/Mar/yyyy:15:32:05 +0900] "GET /fjlogo.gif HTTP/1.1" 200 1647 "http://ihs.fujitsu.com/" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```

Information

Related Directives

- CustomLog
- LoadModule
- LogFormat

3.28 CGI Program Execution Permissions Settings

The execution of CGI programs is enabled using directives such as ScriptAlias or AddHandler.

Examples of setting the directory/extension and enabling the execution of CGI programs are shown below.

- [Setting the CGI program directory](#)
A CGI program directory is set, and the file stored under that directory is executed as a CGI program.
- [Setting the CGI program extension](#)
A CGI program extension is set, and a file with that extension is executed as a CGI program.

Note

- When a request for a CGI program is received, a daemon process is generated (Windows(R)) or a new CGI process from the CGI daemon process is created (Solaris/Linux), and the CGI program is executed on that process. Note that, when the CGI program ends, the CGI process will also end.
- Messages output from the CGI program using standard error output are output to the error log (log level "error").
- **Linux32/64**
Using the CGI program, send the data to standard input and then receive the request message-body. The size of the received request message-body is set in the CONTENT_LENGTH environment variable.
If the size of the request message-body is not received, the following message will be output to the error log, and the response may be slow:

```
(104)Connection reset by peer: ap_content_length_filter: apr_bucket_read() failed
```

- **Solaris32/64** **Linux32/64**
The execution privileges for the user set in the User directive or group set in the Group directive must be set in the CGI program.

Setting the CGI program directory

Example

Windows32/64

Running a file under the "C:\Interstage\F3FMahs\cgi-bin" directory as a CGI program when the specified directory "C:\Interstage\F3FMahs\cgi-bin" is set as the CGI program directory and the URL in the web browser (client) is under "/cgi-bin"

```
LoadModule cgi_module "C:/Interstage/F3FMahs/modules/mod_cgi.so"

ScriptAlias /cgi-bin/ "C:/Interstage/F3FMahs/cgi-bin/"
```

Solaris32/64 Linux32/64

Running a file under the "/opt/FJSVahs/cgi-bin" directory as a CGI program when the specified directory "/opt/FJSVahs/cgi-bin" is set as the CGI program directory and the URL in the web browser (client) is under "/cgi-bin"

```
LoadModule cgid_module "/opt/FJSVahs/modules/mod_cgid.so"

ScriptAlias /cgi-bin/ "/opt/FJSVahs/cgi-bin/"
```

Setting the CGI program extension

Example

Windows32/64

Running a file as a CGI program when the specified extension "cgi" is set as the CGI program extension and the URL in the web browser (client) has file name extension "cgi"

```
LoadModule cgi_module "C:/Interstage/F3FMahs/modules/mod_cgi.so"

<Directory C:/Interstage/F3FMahs/htdocs>
    Options      ExecCGI
    AddHandler  cgi-script .cgi
</Directory>
```

Solaris32/64 Linux32/64

Running a file as a CGI program when the specified extension "cgi" is set as the CGI program extension and the URL in the web browser (client) has file name extension "cgi"

```
LoadModule cgid_module "/opt/FJSVahs/modules/mod_cgid.so"

<Directory /opt/FJSVahs/htdocs>
    Options      ExecCGI
    AddHandler  cgi-script .cgi
</Directory>
```

Information

Related Directives

- AddHandler
- <Directory>
- LoadModule
- Options
- ScriptAlias

- SetHandler

3.29 Access Control for Servlet Service Application URLs

Access control for Servlet service application URLs is set using the <Location> section. Through this setting, the following access control is performed for access requests to the Servlet service application from the web browser:

- User Authentication
- IP Access Control

Here, an example of the IP access control settings is shown.

For details on user authentication, refer to "[3.7 Setting User Authentication](#)". However, the <Directory> section in the environment definition file (httpd.conf) settings example cannot be used, so change this section to the <Location> section so that it can be used.



Example

Allowing access to the Servlet service application URL "/sample" from the specified host "192.168.1.1" only

```
<Location /sample>
  Order Deny,Allow
  Deny from all
  Allow from 192.168.1.1
</Location>
```



Information

Related Directives

- Allow
- Deny
- <Location>
- Order

Chapter 4 Operation and Maintenance

This chapter describes the operation and maintenance of Interstage HTTP Server 2.2.

4.1 Starting and Stopping the Web Server

This section describes starting and stopping the web server.



Solaris32/64 **Linux32/64**

Do not delete the following process management files while operating the web server.

```
/var/opt/FJJSVahs/logs/httpd.pid
```

If the file is deleted, the operation of the web server cannot be guaranteed. Restart the system again to operate normally.

4.1.1 Starting the Web Server

The following methods start the web server:

In the explanation, the default installation path is used as the storage path.

- Start by Using the Service **Windows32/64**
- Start by Using the `httpd` command **Windows32/64**
- Start by Using the `apachectl` command **Solaris32/64** **Linux32/64**
- Start by Using the `httpd` command **Solaris32/64** **Linux32/64**



- Execute this command with administrator authority.

Solaris32/64 **Linux32/64**

To publish content stored on an NFS server, the NFS server must always be accessible while the web server is running. Check that the NFS server has started normally before the web server starts, and do not perform operations that make it impossible to access the NF server while the web server is running (for example, powering off the NFS server).

Start by Using the Service **Windows32/64**

1. Log in with Administrator permission.
2. Open [Control Panel] > [Services] or [Control Panel] > [Administrative Tools] > [Services].
3. Select the following service name and click start.
 - For the default web server: "Interstage HTTP Server 2.2"
 - For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

Start by Using the `httpd` command **Windows32/64**

1. Log in with Administrator permission.

2. Specify the following service name, and execute the `httpd` command to start the web server.

- For the default web server: "Interstage HTTP Server 2.2"
- For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

```
C:\Interstage\F3FMahs\bin\httpd.exe -k start -n "Service name"
```

Start by Using the `apachectl` command Solaris32/64 Linux32/64

Execute the `apachectl` command to start the web server.

- For the default web server:

```
/opt/FJSVahs/bin/apachectl start
```

- For multiple web server operation:

```
<directory containing the web server resources>/bin/apachectl start
```

Start by Using the `httpd` command Solaris32/64 Linux32/64

Execute the `httpd` command to start the web server.

- For the default web server:

```
/opt/FJSVahs/bin/httpd -k start -f /opt/FJSVahs/conf/httpd.conf
```

- For multiple web server operation:

```
/opt/FJSVahs/bin/httpd -k start -f <directory containing the web server resources>/conf/httpd.conf
```

4.1.2 Stopping the Web Server

The following methods stop the web server:

In the explanation, the default installation path is used as the storage path.

- [Stop by Using the Service](#) Windows32/64
- [Stop by Using the `httpd` command](#) Windows32/64
- [Stop by Using the `apachectl` command](#) Solaris32/64 Linux32/64
- [Stop by Using the `httpd` command](#) Solaris32/64 Linux32/64



Note

Execute this command with administrator authority.

Stop by Using the Service Windows32/64

1. Log in with Administrator permission.
2. Open [Control Panel] > [Services] or [Control Panel] > [Administrative Tools] > [Services].
3. Select the following service name and click stop.
 - For the default web server: "Interstage HTTP Server 2.2"

- For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

Stop by Using the httpd command Windows32/64

1. Log in with Administrator permission.
2. Specify the following service name, and execute the [httpd](#) command to stop the web server.
 - For the default web server: "Interstage HTTP Server 2.2"
 - For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

```
C:\Interstage\F3FMahs\bin\httpd.exe -k stop -n "Service name"
```

Stop by Using the apachectl command Solaris32/64 Linux32/64

Execute the [apachectl](#) command to stop the web server.

- For the default web server:

```
/opt/FJSVahs/bin/apachectl stop
```

- For multiple web server operation:

```
<directory containing the web server resources>/bin/apachectl stop
```

Stop by Using the httpd command Solaris32/64 Linux32/64

Execute the [httpd](#) command to stop the web server.

- For the default web server:

```
/opt/FJSVahs/bin/httpd -k stop -f /opt/FJSVahs/conf/httpd.conf
```

- For multiple web server operation:

```
/opt/FJSVahs/bin/httpd -k stop -f <directory containing the web server resources>/conf/httpd.conf
```

4.1.3 Setting Auto Startup

There are two methods of starting the web server: the web server is started automatically when the operating system starts, or is started manually using a command.

The configuration methods for automatic and manual startup are explained below. For details on the procedure to start the web server manually, refer to "4.1.1 Starting the Web Server".

- [Configuration method for automatic startup](#) Windows32/64
- [Configuration method for manual startup](#) Windows32/64
- [Configuration method for automatic startup](#) Solaris32/64 Linux32/64
- [Configuration method for manual startup](#) Solaris32/64 Linux32/64



Note

The automatic startup settings are configured during installation. Change them if necessary.

Configuration method for automatic startup Windows32/64

1. Log in with Administrator permission.
2. Open [Control Panel] > [Services] or [Control Panel] > [Administrative Tools] > [Services].
3. Select the following service name, and change [Startup Type] to [Automatic].
 - For the default web server: "Interstage HTTP Server 2.2"
 - For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

Configuration method for manual startup Windows32/64

1. Log in with Administrator permission.
2. Open [Control Panel] > [Services] or [Control Panel] > [Administrative Tools] > [Services].
3. Select the following service name, and change [Startup Type] to [Manual].
 - For the default web server: "Interstage HTTP Server 2.2"
 - For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

Configuration method for automatic startup Solaris32/64 Linux32/64

Execute the following shell script, and register the startup shell script in the RC procedure.

```
/opt/FJSVahs/etc/boot/ahsautosetup.sh
```

Point

.....
This is registered as the following startup shell script names:

Solaris32/64

- /etc/rc0.d/K17ahs
- /etc/rc1.d/K17ahs
- /etc/rc2.d/K17ahs
- /etc/rc3.d/S51ahs
- /etc/rcS.d/K17ahs

Linux32/64

- /etc/rc0.d/K14ahs
 - /etc/rc1.d/K14ahs
 - /etc/rc2.d/S86ahs
 - /etc/rc3.d/S86ahs
 - /etc/rc4.d/S86ahs
 - /etc/rc5.d/S86ahs
 - /etc/rc6.d/K14ahs
-

Configuration method for manual startup Solaris32/64 Linux32/64

Execute the following shell script, and deregister the startup shell script from the RC procedure.

```
/opt/FJSVahs/etc/boot/ahsautoclean.sh
```

4.1.4 Checking the Status

The method used to check the web server status is shown below.

In the explanation, the default installation path is used as the storage path.



Note

Execute this command with administrator authority.

Windows32/64

1. Log in with Administrator permission.
2. Open [Control Panel] > [Services] or [Control Panel] > [Administrative Tools] > [Services].
3. Check whether "Started" is displayed under [Status] for the following services:
 - For the default web server: "Interstage HTTP Server 2.2"
 - For multiple web server operation: "(Name of the service registered when the web server operating environment is created)"

Solaris32/64 Linux32/64

Using the ps command, check whether the Interstage HTTP Server 2.2 daemon process "httpd" has started.

- For the default web server

```
ps -fp 'cat /opt/FJSVahs/logs/httpd.pid 2>/dev/null' 2> /dev/null
```

- For multiple web server operation

```
ps -fp 'cat <directory containing the web server resources>/logs/httpd.pid 2>/dev/null' 2> /dev/nul
```



Example

Output of ps command

```
UID  PID  PPID  C   STIME TTY   TIME CMD
root 4690  920   0 15:56:49 ?     0:00 /opt/FJSVahs/bin/httpd -k start -f /opt/FJSVahs/conf/httpd.conf
```

4.2 Log

The logs shown below are output in Interstage HTTP Server 2.2.

Access Log

This outputs the access status from the web client.

Error Log

This outputs the error messages that have occurred in the web server.

Trace Log

This collects logs of web client and plug-in module I/O information.

In Interstage HTTP Server 2.2, the output log files can be rotated.

Log file rotation

With log file rotation, when a log file is output and the upper limit for the number of saved log files is exceeded, the oldest log file is deleted before the new file is created. Note that the "last modified" timestamp of the old log file for which rotation was performed is the date/time when the last log file was output before rotation was performed.

Log file operations while the web server is running

While the web server is running, use the following procedure to perform the operation (copy/move/delete/edit) on the oldest log file after the log files have been rotated:

1. When the [environment definition file \(httpd.conf\)](#) directive `ahsrlog` executable statement is specified, specify the `-T`, `-C`, or `-W` option to configure the log file rotation settings. When these options are specified, log file rotation can be performed at the specified date/time, regardless of whether a log is output.
2. Immediately after the date/time specified in the `ahsrlog` executable statement, perform the operation on the old log file.



- Perform the operation on the old log file during a period when access to the web server is light.
- If the maximum log file size is exceeded, for example, log rotation may be performed before the specified date/time. In this case, the logs that should be operated on may be output across multiple log files. Before performing an operation on a log file, consider the operation target log files carefully.
- No operations should be performed on the most recent log file while the web server is running. If operations are performed on the most recent log file, the log file rotation behavior cannot be guaranteed - if an operation was performed by mistake, restart the web server.

Each log that is output in Interstage HTTP Server 2.2 is explained below.

4.2.1 Access Log

In Interstage HTTP Server 2.2, the access status from the web browser is output as a log (access log).

To change the access log output destination or output content, use the environment definition file (`httpd.conf`) to configure these settings. For details on settings, refer to "[3.4 Setting the Access Log](#)".

Output Directory

Access logs are generated in the following directory:

`Windows32/64` (default installation path)

```
C:\Interstage\F3FMahs\logs\accesslog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/accesslog
```



If log file rotation is performed, the access log name is changed from the following initial file name:

```
accesslog.N
```

N: Serial number

N is a serial number beginning at 0. The serial numbers are assigned in order from the latest file, whose serial number is ".0". The serial number of the Nth file is ".(N-1)".



Output Timing

The access log is output when the web server receives a request from the client and sends a response to the client.

Output Format

The output format (ahs-analysis) of an access log is as follows:

Items not specified during access are output as a hyphen ("-").

```
Host-name User-name-identification User-name Date-and-Time "Request" Status-code Data-transfer-capacity Web-Server-IP-address:Port-number Host-header Process-ID Process-time Request-ID
```

Output Items

The details of each output item are as follows:

Output item	Output content
Host-name	IP address or host name of systems such as client or proxy server
User-name-identification	Personal information about a user returned from the client
User-name	User name sent from the client
Date-and-Time	Date/time a request was received from the client The date and time is output in the following format: Format: "[Date/Month/Year:Hour:Minute:Second Time difference from GMT]"
Request	Request content requested by the client
Status-code	Code returned to the client For details about the status code, refer to "Status Codes Reported from the Web Server" chapter of the Messages.
Data-transfer-capacity	Amount of data transferred to the client
Web-Server-IP-address:Port-number	IP address and port number of the web server that receives the request
Host- header	Host header content sent from the client
Process-ID	Process ID of the process that processes the request
Process-time	Time from when the request is received until processing is completed (Micro second)

Output item	Output content
Request-ID	Unique ID granted per request

Output Example

For the year "yyyy"

```
192.168.0.1 - - [16/Jan/yyyy:12:59:02 +0900] "GET / HTTP/1.1" 200 44 192.168.0.2:80 ahs.fujitsu.com
19726 3194 -
```

4.2.2 Error Log

The error status when an error occurs in the web server is output as a log (error log).

To change the error log output destination or output content, use the environment definition file (httpd.conf) to configure these settings. For details on settings, refer to ["3.5 Setting the Error Log"](#).

Output Directory

Error logs are generated in the following directory:

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\logs\errorlog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/errorlog
```



Point

If log file rotation is performed, the error log name is changed from the following initial file name:

```
errorlog.N
```

N: Serial number

N is a serial number beginning at 0. The serial numbers are assigned in order from the latest file, whose serial number is ".0". The serial number of the Nth file is ".(N-1)".

Output Timing

The error log is output when an error occurs in the web server.

Output Format

The output format of an error log is as follows:

```
[Date-and-Time] [Log-level] [client IP-address] (Error-number) Error-explanation: Message-body
```

Output Items

The details of each output item are as follows:

Date-and-Time

Indicates the date and time at which the error occurred.

The date and time is output in the following format:

Format: "[Week Month Date Hour:Minute:Second Year]"

Log-level

Log level	Severity of the error	Output with the default settings
emerg	Emergency error	The error is output.
alert	Fatal error that must be resolved immediately	The error is output.
crit	Error that must be resolved immediately	The error is output.
error	Insignificant error, ignorable	The error is output.
warn	Warning for an ignorable error	The error is output.
notice	Common event to be specially reported	The error is output.
info	Event not reported by notice	The error is not output. (output only when the environment definition is modified)
debug	Event logged during development or debug of a module	The error is not output. (output only when the environment definition is modified)

client IP-address

IP address of systems such as client or proxy server.

This item is output only when an error occurred on the client during access to Interstage HTTP Server 2.2.

This item may be omitted.

Error-number

Indicates the number of an error as assigned in the operating system.

This item may be omitted.

Error-explanation

Brief description of an error.

This item may be omitted.

Message-body

Body of an error message.

For details about the bodies of error messages, refer to "[8.10 Error Log](#)".

Output Example

For the version "x.x" and the year "yyyy"

```
[Thu Mar 7 15:44:11 yyyy] [notice] Interstage HTTP Server 2.2/x.x (Unix) configured -- resuming normal operations
[Thu Mar 7 15:51:01 yyyy] [error] [client 192.168.0.1] File does not exist: /opt/FJSVahs/htdocs/abc
```

4.2.3 Trace Log

The web client and plug-in module I/O information is output as a trace log.

To change the trace log output destination or output content, use the environment definition file (httpd.conf) to configure these settings. For details on settings, refer to "3.6 Setting the Trace Log".

Output Directory

Trace logs are generated in the following directory:

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\logs\tracelog
```

Solaris32/64 (default installation path) **Linux32/64**

```
/var/opt/FJSVahs/logs/tracelog
```

Point

If log file rotation is performed, the trace log name is changed from the following initial file name:

```
tracelog.N
```

N: Serial number

N is a serial number beginning at 0. The serial numbers are assigned in order from the latest file, whose serial number is ".0". The serial number of the Nth file is ".(N-1)".

Output Timing

The trace log is output at the times shown below for each item of trace information.

- Web client I/O information
 - When a TCP connection is established
 - When a TCP connection is closed
 - When an HTTP request is received
 - When an HTTP response is sent
- Plug-in module I/O information
 - When the plug-in module response processing function is called
 - When the plug-in module response processing function is returned

Output Format

The output format of a trace log is as follows:

```
[Date-and-Time][Process-ID][Thread-ID]Event Details-information
```

Output Items

The details of each output item are as follows:

Date-and-Time

Indicates the date and time at which the trace log was output.

The date and time is output in the following format:

Format: "[Date/Month/Year:Hour:Minute:Second.Millisecond]"

Process-ID

Windows32/64

Daemon process ID

Solaris32/64 Linux32/64

Communication process ID

Thread-ID

Communication thread ID

Event Details-information

The trace content formats for each output trigger are shown below.

Output trigger	Event	Detailed information
When a TCP connection is established	conn	IP address of systems such as web client or proxy server:Port number=> IP address of received Web server:Port number
When a TCP connection is closed	disc	
When an HTTP request is received	recv	"Request line" This is replaced with the escaped string before being output.
When an HTTP response is sent	send	Status code
When the plug-in module response processing function is called (Note 1)	call	Module source name (Note 2)
When the plug-in module response processing function is returned (Note 1)	rtn	Module source name (Return code) (Note 2) The following are output as return codes: <ul style="list-style-type: none">- When response processing in this module is not executed: -1- When response processing in this module is executed: Any value except -1

Note 1) The output target plug-in modules are those not provided in Interstage HTTP Server 2.2.

Note 2) This is the source file name when the plug-in module is compiled. The module source name of the web server connector provided in the Interstage Servlet service is output as "mod_jk2.c".



Information

The HTTP Keep-Alive function connection retention time can be checked from the trace log. For the output trace log, the date/time of disc (event when the TCP connection is broken) and send (event when the HTTP response is sent) is checked, and calculated according to the following formula:

$\text{HTTP Keep-Alive function connection retention time} = \text{Date and Time of disc} - \text{Date and Time of send}$

Note) When a timeout occurs for a request from the web server to break the TCP connection to the client, if the disconnection notice from the client cannot be received within two seconds, the connection retention time may be two seconds longer than the setting in the KeepAliveTimeout directive.

.....

Output Example

For the year "yyyy"

```
[04/Mar/yyyy:18:14:12.449][2700][1624]conn 192.168.0.1:2044=>192.168.0.2:80
[04/Mar/yyyy:18:14:12.449][2700][1624]recv "GET / HTTP/1.1"
[04/Mar/yyyy:18:14:12.489][2700][1624]call mod_jk2.c
[04/Mar/yyyy:18:14:12.489][2700][1624]rtn mod_jk2.c(-1)
[04/Mar/yyyy:18:14:12.489][2700][1624]send 200
[04/Mar/yyyy:18:14:12.549][2700][1624]recv "GET /fjlogo.gif HTTP/1.1"
[04/Mar/yyyy:18:14:12.549][2700][1624]call mod_jk2.c
[04/Mar/yyyy:18:14:12.549][2700][1624]rtn mod_jk2.c(-1)
[04/Mar/yyyy:18:14:12.559][2700][1588]conn 192.168.0.1:2045=>192.168.0.2:80
[04/Mar/yyyy:18:14:12.559][2700][1588]recv "GET /interstage.jpg HTTP/1.1"
[04/Mar/yyyy:18:14:12.559][2700][1588]call mod_jk2.c
[04/Mar/yyyy:18:14:12.559][2700][1588]rtn mod_jk2.c(-1)
[04/Mar/yyyy:18:14:12.579][2700][1624]send 200
[04/Mar/yyyy:18:14:12.939][2700][1588]send 200
[04/Mar/yyyy:18:14:12.969][2700][1624]recv "GET /istage_j.gif HTTP/1.1"
[04/Mar/yyyy:18:14:12.969][2700][1624]call mod_jk2.c
[04/Mar/yyyy:18:14:12.969][2700][1624]rtn mod_jk2.c(-1)
[04/Mar/yyyy:18:14:13.120][2700][1624]send 200
[04/Mar/yyyy:18:14:30.973][2700][1588]disc
[04/Mar/yyyy:18:14:31.214][2700][1624]disc
```

4.3 Multiple Web Server Operation

In Interstage HTTP Server 2.2, a web server operating environment can be created to run multiple web servers in addition to the default web server created during the installation.

The procedures to create and delete the web server operating environment are explained below.

4.3.1 Creating the Web Server Operating Environment

The procedure to create the web server operating environment is shown below. In the explanation, the default installation path is used as the storage path.

- [Creating the web server operating environment manually](#) Windows32/64
- [Using a batch file to create the web server operating environment](#) Windows32/64
- [Creating the web server operating environment manually](#) Solaris32/64 Linux32/64
- [Using a shell script to create the web server operating environment](#) Solaris32/64 Linux32/64



.....

Execute this command with administrator authority.

.....

Creating the web server operating environment manually Windows32/64

1. Create a directory used to store web server resources.

Example

For the web server resources directory "C:\servers\www1".

```
mkdir C:\servers\www1
```

- Copy the web server template resource "C:\Interstage\F3FMahs\etc\default etc." to the directory created in 1.

Example

For the web server resources directory "C:\servers\www1".

```
xcopy /e /q /y C:\Interstage\F3FMahs\etc\default\ . C:\servers\www1
```

- Using a text editor, edit the environment definition file "<directory containing the web server resources>\conf\httpd.conf" of the web server template resource that was copied in 2.
Replace the strings, shown below, which are described in the environment definition file (httpd.conf).

String before replacement	String after replacement
@@ServerRoot@@ Note) All locations	Directory containing the web server resources (full path) Note) Use a forward slash ("/") to separate the directories in the path. Example) For the web server resources directory "C:\servers\www1". "C:/servers/www1"
@@Listen@@	Port number of the web server Note) Configure a port number that is different to the default web server port number, and to the port numbers of all services that include the applications on the system.

- Execute the [httpd](#) command to register the service of the web server.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k install -n "Service name" -f "environment definition file (httpd.conf) (full path)"
```

Example

For the service name "Interstage HTTP Server 2.2(web001)", and the web server resources directory "C:\servers\www1".

```
C:\Interstage\F3FMahs\bin\httpd.exe -k install -n "Interstage HTTP Server 2.2(web001)" -f "C:\servers\www1\conf\httpd.conf"
```

- Using a text editor, edit the web server list file "C:\Interstage\F3FMahs\etc\servers.conf".
Add the web server name and the environment definition file (httpd.conf) to the web server list file (servers.conf) as one line, in the following format:

```
web server name=environment definition file (httpd.conf) (full path)
```

Web server name

Specify a maximum of 64 bytes (alphanumerics and hyphens (-)) for the web server (the first and last characters must be alphanumerics). Uppercase and lowercase are treated as being the same.

The web server name is used if linking with the web server connector.

Note

Do not specify a web server name that already exists.

Environment definition file (httpd.conf)

Using a full path, specify the environment definition file (httpd.conf) under the web server resources directory.

Example

For the web server name "web001", and the web server resources directory "C:\servers\www1".

```
FJapache=C:\Interstage\F3FMahs\conf\httpd.conf  
web001=C:\servers\www1\conf\httpd.conf
```

Using a batch file to create the web server operating environment Windows32/64

A batch file is provided to batch execute the procedure above that was created manually.

Execute the batch file in the following format:

```
C:\Interstage\F3FMahs\bin\ahscreateenv.bat <directory containing the web server resources> <port  
number of the web server> <web server name>
```

Directory containing the web server resources

The directory that stores the web server resources is specified using a full path of a maximum of 160 bytes, or the relative path from the current directory that executes this batch file. Even when the directory is specified using a relative path, specify a full path of a maximum of 160 bytes.

Port number of the web server

Specifies the port number of the web server.

Web server name

Specify a maximum of 64 bytes (alphanumerics and hyphens (-)) for the web server (the first and last characters must be alphanumerics). Uppercase and lowercase are treated as being the same. The specified web server name is set in the web server list file (servers.conf).

Note

- An existing directory should not be specified as the web server resources directory.
- Specify a port number that is different to the default web server port number, and to the port numbers of all services that contain the applications on the system.
- An existing web server name cannot be specified as the web server name. Check the web server name set in the web server list file (servers.conf), and ensure that the same web server name is not specified.
- The server name is registered as "Interstage HTTP Server 2.2(web server name)".

Example

For the web server resources directory "C:\servers\www1", the Port number "8080", and the web server name "web001".

```
C:\Interstage\F3FMahs\bin\ahscreateenv.bat "C:\servers\www1" 8080 web001
```

Creating the web server operating environment manually Solaris32/64 Linux32/64

1. Create a directory used to store web server resources.

Example

For the web server resources directory "/servers/www1".

```
mkdir /servers/www1
```

2. Copy the web server template resource "/opt/FJSVahs/etc/default etc." to the directory created in 1.

Example

For the web server resources directory "/servers/www1".

```
cp -pR /opt/FJSVahs/etc/default/. /servers/www1
```

3. Using a text editor, edit the environment definition file "<directory containing the web server resources>conf/httpd.conf" of the web server template resource that was copied in 2.
Replace the strings, shown below, which are described in the environment definition file (httpd.conf).

String before replacement	String after replacement
@@ServerRoot@@ Note) All locations	Directory containing the web server resources (full path)
@@Listen@@	Port number of the web server Note) Configure a port number that is different to the default web server port number, and to the port numbers of all services that include the applications on the system.

4. Using a text editor, edit the environment definition file "<directory containing the web server resources>\bin\apachectl" of the web server template resource that was copied in 2.
Replace the strings, shown below, which are described in the environment definition file (httpd.conf).

String before replacement	String after replacement
@@ServerRoot@@	Directory containing the web server resources (full path)

5. Using a text editor, edit the web server list file "/opt/FJSVahs/etc/servers.conf".
Add the web server name and the environment definition file (httpd.conf) to the web server list file (servers.conf) as one line, in the following format:

```
web server name=environment definition file (httpd.conf) (full path)
```

Web server name

Specify a maximum of 64 bytes (alphanumerics and hyphens (-)) for the web server (the first and last characters must be alphanumerics). Uppercase and lowercase are treated as being different.

The web server name is used if linking with the web server connector.

Note

Do not specify a web server name that already exists.

Environment definition file (httpd.conf)

Using a full path, specify the environment definition file (httpd.conf) under the web server resources directory.

Example

For the web server name "web001", and the web server resources directory "/servers/www1".

```
FJapache=/opt/FJSVahs/conf/httpd.conf
web001=/servers/www1/conf/httpd.conf
```

Using a shell script to create the web server operating environment Solaris32/64 Linux32/64

A shell script is provided to batch execute the procedure above that was created manually.

Execute the shell script in the following format:

```
/opt/FJSVahs/bin/ahscreateenv <directory containing the web server resources> <port number of the web server> <web server name>
```

Directory containing the web server resources

The directory that stores the web server resources is specified using a full path of a maximum of 160 bytes.

Port number of the web server

Specifies the port number of the web server.

Web server name

Specify a maximum of 64 bytes (alphanumerics and hyphens (-)) for the web server (the first and last characters must be alphanumerics). Uppercase and lowercase are treated as being the same. The specified web server name is set in the web server list file (servers.conf).

Note

- An existing directory should not be specified as the web server resources directory.
- Specify a port number that is different to the default web server port number, and to the port numbers of all services that contain the applications on the system.
- An existing web server name cannot be specified as the web server name. Check the web server name set in the web server list file (servers.conf), and ensure that the same web server name is not specified.

Example

For the web server resources directory "/servers/www1", the Port number "8080", and the web server name "web001".

```
/opt/FJSVahs/bin/ahscreateenv /servers/www1 8080 web001
```

4.3.2 Deleting the Web Server Operating Environment

The procedure to delete the web server operating environment is shown below. In the explanation, the default installation path is used as the storage path.

Note

Execute this command with administrator authority.

Windows32/64

1. Stop the web server. For details on stopping the web servers, refer to "4.1.2 Stopping the Web Server".
2. Using the httpd command, delete the target web server service.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k uninstall -n "Service name"
```

Example

For the service name "Interstage HTTP Server 2.2(web001)".

```
C:\Interstage\F3FMahs\bin\httpd.exe -k uninstall -n "Interstage HTTP Server 2.2(web001) "
```

3. Using a text editor, edit the web server list file "C:\Interstage\F3FMahs\etc\servers.conf".
Delete the following line for the target web server from the web server list file (servers.conf):

```
web server name=<directory containing the web server resources>\conf\httpd.conf
```

4. If necessary, delete the target web server resources storage directory.

Solaris32/64 Linux32/64

1. Stop the web server. For details on stopping the Web servers, refer to "4.1.2 Stopping the Web Server".
2. Using a text editor, edit the web server list file "/opt/FJSVahs/etc/servers.conf".
Delete the following line for the target web server from the web server list file (servers.conf):

```
web server name=<directory containing the web server resources>/conf/httpd.conf
```

3. If necessary, delete the target web server resources storage directory.

4.4 Maintenance (Resource Backup and Export)

When using other Interstage services and functions, refer to the "Maintenance (Resource Backup)" chapter in the Operator's Guide, and then back up the Interstage resources, export the resources to another server, or change the server host information.

The backup and export of the Interstage HTTP Server 2.2 resources are explained below.

Point

The tasks for the backup and restore of the Interstage resources can be executed in batch. For details on executing the backup and restore of the Interstage resources in batch, refer to "Collective Maintenance" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide, and then perform the batch operation.

4.4.1 Backup and Export Procedure

The following explains the backup and export procedure for Interstage HTTP Server 2.2 resources.

In the explanation, the default installation path is used as the storage path.

Point

The Interstage HTTP Server 2.2 resources that are backed up or exported will vary depending on the option specified in the `ahsbackup` command. For details on backup/export target resources, refer to table of [backup/export target resources](#) in "7.1 `ahsbackup`".

1. Stop the web server. For details on stopping the web servers, refer to "4.1.2 Stopping the Web Server".
2. Create a directory used to store backup/export resources. Backup/export resources are stored under this directory.

Example

Windows32/64

The following example shows how to backup/export the resources in the "X:\Backup" directory.

```
mkdir X:\Backup
```

Solaris32/64 Linux32/64

The following example shows how to backup/export the resources in the "/backup" directory.

```
mkdir /backup
```

Note

Ensure in advance that the disk on which a backup/export resource directory is to be created has enough free space. The size of disk space required for storing Interstage HTTP Server 2.2 backup/export resources is the total sum of the amounts of backup/export resources.

3. Execute the `ahsbackup` command to back up Interstage HTTP Server 2.2 resources.

Example

Windows32/64

The following example shows how to backup/export the resources in the "X:\Backup\AHS " directory.

```
C:\Interstage\F3FMahs\bin\ahsbackup.exe -d X:\Backup -t all
```

Solaris32/64 Linux32/64

The following example shows how to backup/export the resources in the "/backup/FJSVahs" directory.

```
/opt/FJSVahs/bin/ahsbackup -d /backup -t all
```

Note

For details on `ahsbackup` command , refer to "7.1 `ahsbackup`".

4. Start the web server. For details on starting the web servers, refer to "4.1.1 Starting the Web Server".

4.4.2 Restore and Import Procedure

The following explains the restore and import procedure for Interstage HTTP Server resources.

In the explanation, the default installation path is used as the storage path.

1. Stop the web server. For details on stopping the web servers, refer to "[4.1.2 Stopping the Web Server](#)".
2. Specify the backup directory with the `ahsrestore` command, and restore the Interstage HTTP Server resources 2.2.

Example

Windows32/64

The following example shows how to restore the resources backed up in the "X:\Backup\AHS" directory.

```
C:\Interstage\F3FMahs\bin\ahsrestore.exe -d X:\Backup -t all
```

The following example shows how to import the resources backed up in the "X:\Backup\AHS" directory.

```
C:\Interstage\F3FMahs\bin\ahsrestore.exe -d X:\Backup -t all -h C:\Interstage\F3FMahs\etc\host_table
```

Solaris32/64 Linux32/64

The following example shows how to restore the resources backed up in the "/backup/FJSVahs" directory.

```
/opt/FJSVahs/bin/ahsrestore -d /backup -t all
```

The following example shows how to import the resources backed up in the "/backup/FJSVahs" directory.

```
/opt/FJSVahs/bin/ahsrestore -d /backup -t all -h /etc/opt/FJSVahs/etc/host_table
```

Note

For details on `ahsrestore` command, refer to "[7.2 ahrestore](#)".

3. Start the web server. For details on starting the web servers, refer to "[4.1.1 Starting the Web Server](#)".

Note

If service startup fails after importing the resource, check whether there is a shortage of the imported resources or an error in the importing procedure before taking the action in the output message.

4.5 Cluster Service

To run Interstage HTTP Server 2.2 using the cluster service function, the Interstage environment must be set up on the cluster service.

Set up the Interstage cluster service environment according to the procedure shown below. Refer to the "Environment Setup Procedure for Cluster Service" chapter in the High Availability System Guide, and then set up the Interstage cluster service environment.

1. Installation of Interstage
2. Disabling the Interstage automatic startup setting (**Note**)
3. Cluster System Presetting
4. Interstage Environment Setup (**Note**)
5. Setting of the Cluster System (**Note**)
6. Confirming the Cluster System Behavior (**Note**)

Note) The Interstage HTTP Server 2.2 environment must be set up.

Here, the Interstage HTTP Server 2.2 environment setup for steps 2, 4, 5, and 6 above is explained.



For details on Cluster Service, refer to the "Environment Setup Procedure for Cluster Service" chapter of the High Availability System Guide.

4.5.1 Disabling the Interstage automatic startup setting

In a cluster system, the cluster product will start the Interstage HTTP Server 2.2 web server when the machine starts, so the Interstage HTTP Server 2.2 automatic startup settings must be disabled.

During installation of Interstage HTTP Server 2.2, the settings are configured so that the web server will start automatically. Change the settings so that the web server will not start automatically. For details on setting auto startup, refer to "4.1.3 Setting Auto Startup".

Additionally, stop the web server if it is running. For details on stopping, refer to "4.1.2 Stopping the Web Server".

4.5.2 Interstage HTTP Server 2.2 Environment Setup

To run Interstage HTTP Server 2.2 on a cluster system, store the Interstage HTTP Server 2.2 resources on the active node and standby node local disk using the same resource configuration, and then set up the same environment for each.



Interstage HTTP Server 2.2 only supports 1:1 operation standby. It does not support mutual standby applications.



If the Interstage HTTP Server 2.2 resources (such as the environment definition file or contents file) are stored on a shared disk device, there is no need to set up Interstage HTTP Server 2.2 on the active node and the standby node. The information that was set on the active node will be taken over by the standby node.

4.5.3 Setting the Cluster Service

This section explains the cluster product environment settings that can be used in Interstage. These are shown below. Perform the required environment settings according to the cluster product used.

- **Windows32/64**
userApplication Configuration Wizard
- **Solaris32/64 Linux32/64**
RMS Wizard

For MSCS **Windows32/64**

Using the cluster administrator, register the Interstage HTTP Server 2.2 resources for the cluster system.

Service name	Resource type	Dependent on
- Interstage HTTP Server 2.2	A general-purpose service	- Interstage IP address
- Any service name		- Shared disk (Note)

Note) Set this if the Interstage HTTP Server 2.2 resources (such as the environment definition file or contents file) are stored on a shared disk device.

Note

When registering the Interstage HTTP Server 2.2 service resources, register the resources and then take the action shown below.

- In Windows Server(R) 2008, execute the following command to delete the setup parameters:

```
Cluster Resource "Resource name" /priv StartupParameters=""
```

- In Windows Server(R) 2012, using the failover cluster manager open the [Properties]-[General] tabs of the registered resource, and then delete "startup parameters".

For PRIMECLUSTER Solaris32/64 Linux32/64

For cluster systems, use the Cmdline resource to perform start/stop/switch processing for the service.

Note

In PRIMECLUSTER, the cluster service is "userApplication".

Use the procedure shown below to correct/register the Cmdline resources according to the cluster system operating environment/requirements.

1. Copy the Cmdline resources (samples) under the directory shown below to any directory on the local disk, and then change the file name to "userApplication name.Cmdline resource name". Store the files in the same location on each node.

```
/opt/FJSVahs/etc/HA/PRIMECLUSTER/AHS_INTERSTAGE
```

Point

If Cmdline resources are prepared for each instance, it will be possible to run multiple web server instances.

2. Correct the Cmdline resource items shown below. For details, refer to the PRIMECLUSTER manual.

CONFFILE

Specify the absolute path of the [environment definition file \(httpd.conf\)](#).

PIDFILE

Using the absolute path, specify the value that is set in the PidFile directive of the [environment definition file \(httpd.conf\)](#).

Example

```
# [User Definition]
#
# Please modify following lines, if necessary.
CONFFILE='/opt/FJSVahs/conf/httpd.conf'
PIDFILE='/opt/FJSVahs/logs/httpd.pid'
```

Note

Items not shown above should not be edited.

3. Use the following to register the Cmdline resources in the script:

- **Solaris32/64**
userApplication Configuration Wizard
- **Linux32/64**
RMS Wizard

Example

For Start script

```
>> <Copy destination of Cmdline resources>/AHS_INTERSTAGE start
```

For Stop script

```
>> <Copy destination of Cmdline resources>/AHS_INTERSTAGE stop
```

For Check script

```
>> <Copy destination of Cmdline resources>/AHS_INTERSTAGE status
```

Resource attributes specified when the resource is registered

Item name	Specified value
NULLDETECTOR	No
ALLEXITCODES	No
LIEOFFLINE	No
CLUSTEREXCLUSIVE	Yes
AUTORECOVER	No
MONITORONLY	No
STANDBYCAPABLE	No
REALTIME	No
TIMEOUT	Any (Note)

Note) This is the start and stop timeout (in seconds) of the Cmdline resource. Specify a value which is double the web server start/stop time.

4.5.4 Confirming the Cluster System Behavior

If an error has occurred in Interstage HTTP Server 2.2, check whether cluster nodes have been switched.

Run the tests shown below to cause the error, and check whether cluster nodes have been switched. Additionally, after the cluster nodes have been switched, use a command, for example, to check whether Interstage HTTP Server 2.2 runs correctly on the active node and standby node.

Windows32/64

1. On the active node, identify the process ID using the pid file that is set in the PidFile directive of the [5.5.1 Environment Definition File \(httpd.conf\)](#)

2. Using Task Manager, end the process in step 1.

Solaris32/64 Linux32/64

On the active node, end the process using the following command:

```
# kill -9 `cat /opt/FJShVahs/logs/httpd.pid`
```

Note

- "-9" must be specified as the signal that is sent to the kill command.
- In the cat command, specify the pid file that is set in the PidFile directive of the [5.5.1 Environment Definition File \(httpd.conf\)](#).

4.6 Security Measures

This section describes the following topics:

- [Notes When Making Access](#)
- [Notes on Communication Data](#)
- [Unauthorized Access to Resource Files](#)
- [Leakage of Password Information](#)
- [Threats of Denial of Service Attacks \(DoS\)](#)
- [Risk of Exploiting the HTTP TRACE Method](#)
- [Threat that the Account Name will be Discovered](#) **Solaris32/64 Linux32/64**

Notes When Making Access

When accessing the web server from a web browser, there is a threat that a malicious user will impersonate another user having valid access permissions to the web server.

To prevent this, SSL encryption using SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) client authentication is recommended.

For information about SSL encryption, refer to the "[3.10 Setting the SSL](#)".

Notes on Communication Data

An ill-intentioned person could access communication data between the server and a user who has proper access permission.

SSL encryption is recommended in order to minimize this type of risk.

For information about SSL encryption, refer to the "[3.10 Setting the SSL](#)".

Unauthorized Access to Resource Files

Interstage HTTP Server 2.2 has resource files listed below:

- Contents
- Environment definition file (httpd.conf)
- Web server list file (servers.conf)
- Access log file

- Error log file
- Trace log file
- CGI
- Environment definition file for each directory (.htaccess)

These files may be exposed to the threat of unauthorized access.

To protect these files, make these files inaccessible by end users. Making this file accessible only to users with administrator privileges is recommended (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

Leakage of Password Information

The Interstage HTTP Server 2.2 has a password file, which an ill-intentioned person may furtively look into.

The password data in the password file is encrypted; still, it is recommended that the administrator create the password file using the `htpasswd` command to make it inaccessible by end users. For details on how to create the password file, refer to "[3.7 Setting User Authentication](#)"

Threats of Denial of Service Attacks (DoS)

An ill-intentioned person on the network could target a server and disable its services. To defend the server from Denial of Service attacks (DOS), it is recommended to use the following functions:

- User authentication:

For information about user authentication, refer to "[3.7 Setting User Authentication](#)".

- IP access control:

It is possible to permit access only to specific clients.

For information about IP access control, refer to "[3.8 Setting IP Access Control](#)".

- Use of SSL encryption:

High level of security can be retained, where client authentication is possible.

For information about SSL encryption, refer to the "[3.10 Setting the SSL](#)".

- Limitations on the size of request message from client:

Set the maximum size of a request message to prevent a buffer overflow. The maximum size of the request message is set by the following directives of the environmental definition file (httpd.conf):

- LimitRequestBody
- LimitRequestFields
- LimitRequestFieldsize
- LimitRequestLine

Risk of Exploiting the HTTP TRACE Method

Malicious users (or machines) on the network may read private information in HTTP request data or execute unwanted codes.

To prevent this risk, it is recommended that the TraceEnable directive in the environment definition file (httpd.conf) be set to "off", and the HTTP TRACE method be disabled.

The TRACE method is the HTTP/1.1 method of receiving the data sent from the client side as response data. This method is used to diagnose the network environment. There is no problem in the web server operation if this method is disabled because it not usually used.

```
TraceEnable off
```

Threat that the Account Name will be Discovered Solaris32/64 Linux32/64

There is always a risk that an account name on the web server will be discovered on the network by a user (or machine) with malicious intent.

To counter this kind of threat, it is recommended that the settings in the environment settings file (httpd.conf) are made as shown below. These settings will disable requests to documents under the account user home directory.

```
LoadModule userdir_module "/opt/FJSVahs/modules/mod_userdir.so"
UserDir disabled
```

Point

A hash mark (#) can be added to the start of the LoadModule and UserDir directives to make the line a comment.

To make a document under the account user home directory public, configure the following settings:

- Set the access authority in the home directory to be made public for access from the web server.
- Disable the user directory settings for users that are not going to be made public.

An example of disabling the user directory settings for users that are not going to be made public is shown below.

Example

Making "user1" and "user2" documents under "user home directory/public_html" public.

```
LoadModule userdir_module "/opt/FJSVahs/modules/mod_userdir.so"
UserDir public_html
UserDir disabled
UserDir enabled user1 user2
```

Making all documents, except for "user3" and "user4", under "user home directory/public_html" public.

```
LoadModule userdir_module "/opt/FJSVahs/modules/mod_userdir.so"
UserDir public_html
UserDir disabled user3 user4
```

Note

If just "UserDir public_html" is specified, when the "http://host name[:port number]/~user" request is received, the status code that is returned when the user name is specified as "user" depends on whether the user exists in the Solaris/Linux server. For this reason, the account name on the web server might be discovered. These status codes are shown below.

- "user" does not exist:
The "404 Not Found" status code is returned.
- "user" exists:
The "403 Forbidden" status code is returned.

This status code is returned because, although "user" exists, access authority for access from the web server for this user has not been set in the home directory. Specify users that can execute the web server in the User directive.

Linux32/64

This problem occurs when the user home directory is created using the useradd command, and directory authority is only set for the owner, meaning that only that user has access permission.

4.7 IPv6 Communication

In Interstage HTTP Server 2.2, HTTP/HTTPS communication can be performed in IPv6 environments. The port number is specified and set in the Listen directive of the environment definition file (httpd.conf).

4.8 Restrictions

Some functions described in this manual have restrictions. The following tables detail these restrictions.

No	Restriction	Remarks	Date of Removal
1	When a certificate in UTF-8 format, (such as a CA certificate, site certificate, or client certificate) is used for SSL communication, the following restrictions apply: - When SSL protocol Version 3 (client certificate) is used, the CA certificate and the client certificate in UTF-8 must be registered on both the Interstage HTTP Server 2.2 and the web browser. - When SSL protocol Version 2 (server authentication) is used, the CA certificate and the client certificate in UTF-8 must be registered on both the Interstage HTTP Server 2.2 and the web browser.	None	Not determined
2	Solaris32/64 Linux32/64 To link with the web server connector, the value set in the ThreadsPerChild directive of the environment definition file (httpd.conf) should not be changed from "1".	None	Not determined

4.9 Notes

This section describes notes on the Interstage HTTP Server 2.2.

- [Privileges for using Interstage HTTP Server 2.2](#) **Windows32/64**
- [Operating Web Server](#) **Solaris32/64 Linux32/64**
- [Third Party plug-in Module Support](#)
- [Certificates Issued using OpenSSL](#)
- [HTTP Methods for Static Content](#)
- [CGI Programs](#) **Linux32/64**
- [Firewall Setting](#) **Windows32/64 Linux32/64**

Privileges for using Interstage HTTP Server 2.2 **Windows32/64**

The following operations can be used only by Administrators or by users who belong to the Administrators group:

- Web server start

- Web server stop

Operating Web Server Solaris32/64 Linux32/64

Do not delete the following process management files while operating the web server.

```
/var/opt/FJSVahs/logs/httpd.pid
```

If the file is deleted, the operation of the web server cannot be guaranteed. Restart the system again to operate normally.

Third Party plug-in Module Support

Third party plug-in modules, including mod_perl and mod_php, are not supported - only plug-in modules provided in the Fujitsu product can be used.

If a non-unsupported plug-in module is installed in Interstage HTTP Server 2.2, then none of the Interstage HTTP Server 2.2 operations will be supported.

Certificates Issued using OpenSSL

Certificates issued using OpenSSL cannot be used. For details on certificates, refer to the Security System Guide.

HTTP Methods for Static Content

The HTTP methods below can be used for static content (POST method cannot be used):

- GET
- HEAD
- OPTIONS
- TRACE

CGI Programs Linux32/64

Using a CGI program, input using standard input and then receive the request message body text. The received request message body text size is the size set in the CONTENT_LENGTH environment variable.

If the request message body text is not received, the following message will be output to the error log, and the response may be slow:

```
(104)Connection reset by peer: ap_content_length_filter: apr_bucket_read() failed
```

Firewall Settings Windows32/64 Linux32/64

The access to the web server may fail if a firewall is enabled. Take the steps detailed below to change the system settings, removing firewall blocks.

Step to remove firewall blocks Windows32/64

1. Open [Windows Firewall] from the [Control Panel].
2. Click [General], and set [Enable (recommended)] to [On]. Check that the [Do not allow exceptions] checkbox is not selected.
3. Click [Exception], and then click [Add Programs].

4. Click [Browse], select the following file, and then click [Open].

```
C:\Interstage\F3FMahs\bin\httpd.exe
```

5. Click [OK] in the [Add Programs] window.
6. In the [Programs and Services] list, select the checkbox for the program added in step 4, and then click [OK].

Step to remove firewall blocks (For RHEL5) Linux32/64

1. In the [System] menu, select [Manage] and open [Security Level and Firewall Settings].
2. If [Firewall] in the [Firewall Option] tab is disabled, no action is required. If it is enabled, take the steps detailed below.
3. In the [Firewall Options] tab, open [Other Port].
4. Click [Add], and enter the port number of the Interstage HTTP Server 2.2 in the [Port Addition] window. Leave Protocol as the default, "tcp" and click [OK].
5. In the Security Level Settings screen, click [OK].

Step to remove firewall blocks (For RHEL6) Linux32/64

1. In the [System] menu, select [Administration] and click [Firewall].
2. Click [Other Ports] in the [Firewall Configuration] window.
3. Click [Add] - the [Port and Protocol] window will be displayed.
4. Select "User Defined" and enter the port number of the Interstage HTTP Server 2.2 in the "Port / Port Range".
5. Enter "tcp" (the default value) as the protocol and click [OK].
6. Click [Apply].
7. In the [File] menu, select [Quit].

Chapter 5 Tuning

This chapter describes Interstage HTTP Server 2.2 tuning.

5.1 Disk Space Requirements

This section describes the disk space requirements for the following items:

Directory	Disk space (MB)	Remarks
Access log, error log, and trace log directory	Determine the required size from operation details.	Access log, error log, and trace log
Contents directory	Determine the required size from operation details.	Contents (for example, HTML documents)

5.2 Memory Requirements

This section describes the memory requirements.



Note

If there is insufficient memory to run the web server, problems may occur in the behavior of the web server.

Memory (MB)	
Windows32/64	$13.9 + (0.18 * m)$ or more
Solaris32/64	$20.0 + (5.0 * n / m) + (0.1 * n)$ or more
Linux32/64	$5.5 + (5.0 * n / m) + (0.1 * n)$ or more

m: The value set for the ThreadsPerChild directive in the environment definition file (httpd.conf).

n: The value set for the MaxClients directive in the environment definition file (httpd.conf).

5.3 System Resource Requirements (Solaris)

When running Interstage HTTP Server 2.2, it may be necessary to extend the number of file descriptors depending on the functions used in the web server and the content defined in the environment definition file (httpd.conf).

Refer to the following table before calculating the value to be set for the required number of file descriptors.

System resources	Parameter	Required amount
Maximum number of file descriptor	[For /etc/system] rlim_fd_cur	m + 10 or more
	[For resource control] process.max-file-descriptor	[When the following features are used] Add the following values to the above: - Basic Authentication function: m - SSL communication: 21 - Proxy function: m

System resources	Parameter	Required amount
		- CGI function (Note): 1
		[When the following directives are added to the environment definition file (httpd.conf)] Add the following values to the above: - CustomLog(specify " command execution statement"): 2 * directive number - CustomLog(specify file name): 1* directive number - ErrorLog: 2 * directive number - Listen: 2 * directive number

m: The value set for the ThreadsPerChild directive in the environment definition file (httpd.conf).

Note) Also add the number of file descriptors that are required in the CGI program that is to be run.

If the value calculated above exceeds the system default value, change the system parameter value according to the procedure shown below.

Changing the System Parameters (for the /etc/system file)

The procedure to change the system parameter using r the /etc/system file is shown below. For details, refer to the relevant document for the operating system.

1. Edit /etc/system file. Change the parameter value in the /etc/system file to the value calculated above.
2. Restart the operating system.

Changing the System Parameters (for resource control)

The procedure to change the system parameter using resource control is shown below. For details, refer to the relevant document for the operating system.

1. Stop the web server. For details on stopping the web servers, refer to "4.1.2 Stopping the Web Server".
2. Using the projmod command, change the user.root project and system project parameters.



Example

When the privilege level to be changed is "privileged", and the action following a request where the threshold setting was exceeded is "deny"

```
projmod -s -K 'process.max-file-descriptor=(privileged,1024,deny)' user.root
projmod -s -K 'process.max-file-descriptor=(privileged,1024,deny)' system
```

3. Reflect the value that was changed using the newtask command.

```
newtask -p user.root -c $$
```

4. Start the web server. For details on starting the web servers, refer to "4.1.1 Starting the Web Server".

5.4 System Resource Requirements (Linux)

When running Interstage HTTP Server 2.2, it may be necessary to extend the number of semaphores and file descriptors depending on the functions used in the web server and the content defined in the environment definition file (httpd.conf).

Refer to the following table before calculating the value to be set for the required number of semaphores and file descriptors.

System resources		Parameter	Type	Required amount
Semaphores	Maximum number of semaphores for each semaphore ID	[System Parameters (/etc/sysctl.conf)] <i>para1</i> (kernel.sem)	Setting value	1 or more
	Number of semaphores of the entire system	[System Parameters (/etc/sysctl.conf)] <i>para2</i> (kernel.sem)	Additional value (Note 1)	1 or more
	Maximum number of operations for each semaphore call	[System Parameters (/etc/sysctl.conf)] <i>para3</i> (kernel.sem)	Setting value	1 or more
	Maximum number of semaphore IDs	[System Parameters (/etc/sysctl.conf)] <i>para4</i> (kernel.sem)	Additional value (Note 1)	1 or more
Maximum number of file descriptor	Maximum number of file descriptors in the entire system	[System Parameters (/etc/sysctl.conf)] fs.file-max	Additional value (Note 1)	n + 10 or more
				[When the following features are used] Add the following values to the above: <ul style="list-style-type: none"> - Basic Authentication function: n - SSL communication: 21 * n / m - Proxy function: n - CGI function (Note 2): 13 + n / m [When the following directives are added to the environment definition file (httpd.conf)] Add the following values to the above: <ul style="list-style-type: none"> - CustomLog(specify " command execution statement"): 2 * directive number * n / m - CustomLog(specify file name): 1 * directive number * n / m - ErrorLog: 2 * directive number * n / m - Listen: 2 * directive number * n / m
Maximum number of file descriptors that can be opened by the user	Maximum number of file descriptors that can be opened by the user	[Resource control (/etc/security/limits.conf)] nofile	Setting value	m + 10 or more
				[When the following features are used] Add the following values to the above: <ul style="list-style-type: none"> - Basic Authentication function: m

System resources		Parameter	Type	Required amount
				<ul style="list-style-type: none"> - communication: 21 - Proxy function: m - CGI function (Note 2): 1
				<p>[When the following directives are added to the environment definition file (httpd.conf)]</p> <p>Add the following values to the above:</p> <ul style="list-style-type: none"> - CustomLog(specify " command execution statement"): 2 * directive number - CustomLog(specify file name): 1 * directive number - ErrorLog: 2 * directive number - Listen: 2 * directive number

m: The value set for the ThreadsPerChild directive in the environment definition file (httpd.conf).

n: The value set for the MaxClients directive in the environment definition file (httpd.conf).

Note 1) When multiple web servers are running, add the required number for each web server.

Note 2) Also add the number of file descriptors that are required in the CGI program that is to be run.

If the value calculated above exceeds the system default value, change the system parameter value according to the procedure shown below.

Changing the System Parameters (for /etc/sysctl.conf)

The procedure to change the system parameter is shown below. For details, refer to the document of the operating system.

1. Edit /etc/sysctl.conf file.

If the "Type" field in the above table is "Setting value", change the parameter value in the /etc/sysctl.conf file to the value calculated above.

If the "Type" field in the above table is "Additional value", add the value calculated above to the parameter value in the /etc/sysctl.conf file.



The parameter of the semaphore is specified in the following format.

```
kernel.sem = para1 para2 para3 para4
```

2. Execute the following command. Or, Restart the operating system.

```
sysctl -p /etc/sysctl.conf
```

Changing the Resource Control (for /etc/security/limits.conf)

The procedure to control the system resource is shown below. For details, refer to the document of the operating system.

1. Edit /etc/security/limits.conf file. Change the parameter value in the /etc/security/limits.conf file to the value calculated above.
2. Restart the operating system.

5.5 Environment Definition

In Interstage HTTP Server 2.2, define the environment using the following files:

Files

[Environment Definition File \(httpd.conf\)](#)

[Web Server List File \(servers.conf\)](#)

5.5.1 Environment Definition File (httpd.conf)

Overview

The httpd.conf file contains definitions relating to Interstage HTTP Server 2.2 operating environments.

Storage directory

For the default web server

Windows32/64 (default installation path)

```
C:\Interstage\F3FMahs\conf\httpd.conf
```

Solaris32/64 (default installation path) **Linux32/64**

```
/etc/opt/FJSVahs/conf/httpd.conf
```

For multiple web server operation

Windows32/64

```
<directory containing the web server resources>\conf\httpd.conf
```

Solaris32/64 **Linux32/64**

```
<directory containing the web server resources>/conf/httpd.conf
```



Note

- "Default web server" above refers to the web server created during installation.
- "Multiple web server operation" above refers to the web server created after the installation in order to run multiple web servers.
- If this file is edited, the changes will be effective the next time the web server starts.

File Contents

Using a text editor, configure the web server operating environment using the relevant directives. According to the settings in this file, various function requests will be supported for the web server.

For details on directives that can be configured, refer to "[Chapter 6 Directives](#)".

Point

- A comment line starts with a number sign ("#").
- Use a maximum of 8191 bytes per string per line.

5.5.2 Web Server List File (servers.conf)

Overview

The servers.conf file is used to set the web server list for running multiple web servers.

The web server list set in this file is used in the operation of the following functions:

- Web Server Connector (for Interstage HTTP Server 2.2)
- Backup command ([ahsbackup](#))
- [Solaris32/64](#) [Linux32/64](#)
Automatic startup of the web server when the operating system starts
- Batch information collection tool ([iscollectinfo](#))

Storage directory

[Windows32/64](#) (default installation path)

```
C:\Interstage\F3FMahs\etc\servers.conf
```

[Solaris32/64](#) (default installation path) [Linux32/64](#)

```
/etc/opt/FJSVahs/etc/servers.conf
```

Note

The file name and storage directory of this file cannot be changed.

File Contents

To run multiple web servers, set the web server list using a text editor.

During installation, the default web server "FJapache" line shown below is defined as the first line.

[Windows32/64](#) (default installation path)

```
FJapache=C:\Interstage\F3FMahs\conf\httpd.conf
```

[Solaris32/64](#) (default installation path) [Linux32/64](#)

```
FJapache=/opt/FJSVahs/conf/httpd.conf
```

When creating the web server operating environment, add the web server name and environment definition file (httpd.conf) to the next web server line that has already been defined. Use the following format. Additionally, when deleting the web server operating environment, delete the following line for the associated web server.

```
web server name=environment definition file (httpd.conf) (full pathname)
```

Setting Example

Windows32/64

When creating the web server operating environment, setting the web server name "web001" and a web server with the web server resources storage directory "C:\servers\www1"

```
FJapache=C:\Interstage\F3FMahs\conf\httpd.conf  
web001=C:\servers\www1\conf\httpd.conf
```

Solaris32/64 Linux32/64

When creating the web server operating environment, setting the web server name "web001" and a web server with the web server resources storage directory "/servers/www1"

```
FJapache=/opt/FJSVahs/conf/httpd.conf  
web001=/servers/www1/conf/httpd.conf
```

Chapter 6 Directives

The list of directives that can be configured in Interstage HTTP Server 2.2 is shown below.

Refer to the "Apache HTTP Server Version 2.2 Documentation" for details on the Apache HTTP Server Version 2.2.22 offer directive.

Point

This list of directives is comprised of:

- Directives provided in Apache HTTP Server Version 2.2.22 which can be configured in Interstage HTTP Server 2.2
- Directives provided in Interstage HTTP Server 2.2 (explained in "Additional explanation about the directive" in the table below)

Directive Index

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#)

Directive List

	Directive	Remarks
A	AcceptFilter	
	AcceptMutex	
	AcceptPathInfo	
	AccessFileName	
	Action	
	AddAlt	
	AddAltByEncoding	
	AddAltByType	
	AddCharset	
	AddDefaultCharset	
	AddDescription	
	AddEncoding	
	AddHandler	
	AddIcon	
	AddIconByEncoding	
	AddIconByType	
	AddInputFilter	
	AddLanguage	
	AddModuleInfo	
	AddOutputFilter	
	AddOutputFilterByType	
AddType		
Alias		
AliasMatch		

	Directive	Remarks
	Allow	
	AllowCONNECT	
	AllowEncodedSlashes	
	AllowOverride	
	Anonymous	
	Anonymous_LogEmail	
	Anonymous_MustGiveEmail	
	Anonymous_NoUserID	
	Anonymous_VerifyEmail	
	AuthBasicAuthoritative	
	AuthBasicProvider	
	AuthDBDUserPWQuery	
	AuthDBDUserRealmQuery	
	AuthDBMGroupFile	
	AuthDBMType	
	AuthDBMUserFile	
	AuthDefaultAuthoritative	
	AuthDigestAlgorithm	
	AuthDigestDomain	
	AuthDigestNonceLifetime	
	AuthDigestProvider	
	AuthDigestQop	
	AuthDigestShmemSize	
	AuthGroupFile	(Note 1)
	AuthName	
	<AuthnProviderAlias>	
	AuthType	
	AuthUserFile	
	AuthzDBMAuthoritative	
	AuthzDBMType	
	AuthzDefaultAuthoritative	
	AuthzGroupFileAuthoritative	
	AuthzOwnerAuthoritative	
	AuthzUserAuthoritative	
B	BalancerMember	
	BrowserMatch	
	BrowserMatchNoCase	
	BufferedLogs	
C	CacheDefaultExpire	

	Directive	Remarks
	CacheDirLength	
	CacheDirLevels	
	CacheDisable	
	CacheEnable	
	CacheIgnoreCacheControl	
	CacheIgnoreHeaders	
	CacheIgnoreNoLastMod	
	CacheIgnoreQueryString	
	CacheIgnoreURLSessionIdentifiers	
	CacheLastModifiedFactor	
	CacheLock	
	CacheLockMaxAge	
	CacheLockPath	
	CacheMaxExpire	
	CacheMaxFileSize	
	CacheMinFileSize	
	CacheNegotiatedDocs	
	CacheRoot	(Note 2)
	CacheStoreNoStore	
	CacheStorePrivate	
	CGIMapExtension	
	CharsetDefault	
	CharsetOptions	
	CharsetSourceEnc	
	CheckCaseOnly	
	CheckSpelling	
	ChrootDir	
	ContentDigest	
	CookieDomain	
	CookieExpires	
	CookieLog	
	CookieName	
	CookieStyle	
	CookieTracking	
	CoreDumpDirectory	
	CustomLog	The ahsrlog execution statement can be specified for pipe of the CustomLog directive.
D	Dav	
	DavDepthInfinity	
	DavGenericLockDB	

	Directive	Remarks
	DavLockDB	
	DavMinTimeout	
	DBDExptime	
	DBDKeep	
	DBDMax	
	DBDMin	
	DBDParams	
	DBDPersist	
	DBDPrepareSQL	
	DBDriver	
	DefaultIcon	
	DefaultLanguage	
	DefaultType	
	DeflateBufferSize	
	DeflateCompressionLevel	
	DeflateFilterNote	
	DeflateMemLevel	
	DeflateWindowSize	
	Deny	
	<Directory>	
	DirectoryIndex	
	<DirectoryMatch>	
	DirectorySlash	
	DocumentRoot	(Note 3)
	DumpIOInput	
	DumpIOLogLevel	
	DumpIOOutput	
E	EnableExceptionHook	
	EnableMMAP	
	EnableSendfile	
	ErrorDocument	(Note 4)
	ErrorLog	The ahrslog execution statement can be specified for pipe of the ErrorLog directive. (Note 5)
	ExpiresActive	
	ExpiresByType	
	ExpiresDefault	
	ExtendedStatus	
	ExtFilterDefine	
	ExtFilterOptions	

	Directive	Remarks
F	FallbackResource	
	FileETag	(Note 6)
	<Files>	
	<FilesMatch>	
	FilterChain	
	FilterDeclare	
	FilterProtocol	
	FilterProvider	
	FilterTrace	
	ForceLanguagePriority	
	ForceType	
	ForensicLog	
	G	GprofDir
GracefulShutdownTimeout		
Group		
H	Header	
	HeaderName	
	HostnameLookups	
I	IdentityCheck	
	IdentityCheckTimeout	
	<IfDefine>	
	<IfModule>	
	<IfVersion>	
	ImapBase	
	ImapDefault	
	ImapMenu	
	Include	
	IndexHeadInsert	
	IndexIgnore	
	IndexOptions	
	IndexOrderDefault	
	IndexStyleSheet	
	ISAPIAppendLogToErrors	
	ISAPIAppendLogToQuery	
	ISAPICacheFile	
	ISAPIFakeAsync	
	ISAPILogNotSupported	
	ISAPIReadAheadBuffer	
ISSsoBusinessSystemName	Interstage HTTP Server 2.2 provide directive	

	Directive	Remarks
K	KeepAlive	
	KeepAliveTimeout	The number of seconds that web server will wait for a subsequent request before closing the connection: 0 - 2147483647 (second) If "0" is specified, the connection is broken immediately after the initial request has been processed.
L	LanguagePriority	
	<Limit>	
	<LimitExcept>	
	LimitInternalRecursion	Range specified for the maximum number of internal redirections/ subrequests: 1 - 2147483647 (Note 7)
	LimitRequestBody	
	LimitRequestFields	Range specified for the maximum number of fields: 0 - 2147483647
	LimitRequestFieldSize	Range specified for the maximum size of each field: 0 - 2147483647 (bytes)
	LimitRequestLine	Range specified for the maximum size of the HTTP request line: 0 - 2147483647 (bytes)
	LimitXMLRequestBody	
	Listen	Specifiable value of port number: 1 - 65535 (Note 8)
	ListenBackLog	(Note 9)
	LoadFile	
	LoadModule	
	<Location>	
	<LocationMatch>	
	LockFile	
	LogFormat	
LogLevel		
M	MaxClients	
	MaxKeepAliveRequests	Specifiable value of Request number: 0 - 2147483647 (Note 10)
	MaxMemFree	
	MaxRanges	Range specified for the maximum number of specified HTTP ranges: 1 - 2147483647 (Note 11)
	MaxRequestsPerChild	Specifiable value of HTTP Request number: 0 - 2147483647 (Note 12)
	MaxRequestsPerThread	
	MaxSpareThreads	
	MCacheMaxObjectCount	
	MCacheMaxObjectSize	

	Directive	Remarks
	MCacheMaxStreamingBuffer	
	MCacheMinObjectSize	
	MCacheRemovalAlgorithm	
	MCacheSize	
	MetaDir	
	MetaFiles	
	MetaSuffix	
	MIMEMagicFile	
	MinSpareThreads	
	ModMimeUsePathInfo	
	MultiviewsMatch	
N	NameVirtualHost	Specifiable value of Port number: "*" or 1 - 65535 If "*" is specified for the port number, or the port number is omitted, all port numbers will be targets.
	NoProxy	
O	Options	
	Order	
P	PassEnv	
	PidFile	
	Protocol	
	<Proxy>	
	ProxyBadHeader	
	ProxyBlock	
	ProxyDomain	
	ProxyErrorOverride	
	ProxyFtpDirCharset	
	ProxyIOBufferSize	
	<ProxyMatch>	
	ProxyMaxForwards	
	ProxyPass	
	ProxyPassInterpolateEnv	
	ProxyPassMatch	
	ProxyPassReverse	
	ProxyPassReverseCookieDomain	
	ProxyPassReverseCookiePath	
	ProxyPreserveHost	
	ProxyReceiveBufferSize	
	ProxyRemote	
	ProxyRemoteMatch	
	ProxyRequests	

	Directive	Remarks
	ProxySCGIInternalRedirect	
	ProxySCGISendfile	
	ProxySet	
	ProxyStatus	
	ProxyTimeout	
	ProxyVia	
R	ReadmeName	
	ReceiveBufferSize	
	Redirect	
	RedirectMatch	
	RedirectPermanent	
	RedirectTemp	
	RemoveCharset	
	RemoveEncoding	
	RemoveHandler	
	RemoveInputFilter	
	RemoveLanguage	
	RemoveOutputFilter	
	RemoveType	
	RequestHeader	
	RequestReadTimeout	
	Require	
	RewriteBase	
	RewriteCond	
	RewriteEngine	
	RewriteLock	
	RewriteLog	
	RewriteLogLevel	
	RewriteMap	
	RewriteOptions	
	RewriteRule	
	RLimitCPU	
	RLimitMEM	
	RLimitNPROC	
S	Satisfy	
	ScoreBoardFile	
	Script	
	ScriptAlias	
	ScriptAliasMatch	

Directive	Remarks
ScriptInterpreterSource	
ScriptLog	
ScriptLogBuffer	
ScriptLogLength	
ScriptSock	
SeeRequestTail	
SendBufferSize	Specifiable value of Buffer size: 0 or 512 - 2147483647 (Note 13)
ServerAdmin	
ServerAlias	
ServerLimit	(Note 14)
ServerName	(Note 15)
ServerPath	
ServerRoot	
ServerSignature	
ServerTokens	
SetEnv	
SetEnvIf	
SetEnvIfNoCase	
SetHandler	
SetInputFilter	
SetOutputFilter	
SSIEnableAccess	
SSIEndTag	
SSIErrorMsg	
SSIETag	
SSILastModified	
SSIStartTag	
SSITimeFormat	
SSIUndefinedEcho	
SSLCertExpand	Interstage HTTP Server 2.2 provide directive
SSLCertExpire	Interstage HTTP Server 2.2 provide directive
SSLCertName	Interstage HTTP Server 2.2 provide directive
SSLCICACertName	Interstage HTTP Server 2.2 provide directive
SSLCipherSuite	Interstage HTTP Server 2.2 provide directive
SSLConfName	Interstage HTTP Server 2.2 provide directive
SSLEnvDir	Interstage HTTP Server 2.2 provide directive
SSLExec	Interstage HTTP Server 2.2 provide directive
SSLHandshakeTimeout	Interstage HTTP Server 2.2 provide directive

	Directive	Remarks
	SSLLIBMultiSession	Interstage HTTP Server 2.2 provide directive
	SSLMaxSession	Interstage HTTP Server 2.2 provide directive
	SSLNotifyVers	Interstage HTTP Server 2.2 provide directive
	SSLSlotDir	Interstage HTTP Server 2.2 provide directive
	SSLTokenLabel	Interstage HTTP Server 2.2 provide directive
	SSLUserPINFile	Interstage HTTP Server 2.2 provide directive
	SSLVerifyClient	Interstage HTTP Server 2.2 provide directive
	SSLVersion	Interstage HTTP Server 2.2 provide directive
	StartServers	
	Substitute	
	Suexec	
	SuexecUserGroup	
T	ThreadLimit	
	ThreadsPerChild	Specifiable value of Client number: 1 - Value set for the ThreadLimit directive (Note 16)
	ThreadStackSize	
	TimeOut	Specifiable value of Response time: 0 - 2147483647 (Minute)
	Trace	Interstage HTTP Server 2.2 provide directive
	TraceEnable	
	TraceLog	Interstage HTTP Server 2.2 provide directive
	TransferLog	
U	TypesConfig	
	UnsetEnv	
	UseCanonicalName	
	UseCanonicalPhysicalPort	
	User	
UserDir		
V	VirtualDocumentRoot	
	VirtualDocumentRootIP	
	<VirtualHost>	
	VirtualScriptAlias	
	VirtualScriptAliasIP	
W	Win32DisableAcceptEx	
X	XBitHack	

6.1 Notes on the Directives

This section contains notes on the use of the directives.



In this manual and "Apache HTTP Server Version 2.2 Documentation", there may be differences in directive names depending on whether uppercase and lowercase is used. However, this does not pose a problem because directive names are not case-sensitive.

Note 1) Notes on AuthGroupFile directive

- In the group file specified in the AuthGroupFile directive, define the group name and user name using a maximum of 8,191 bytes per line. If a string longer than this is defined on a line, all bytes that exceed the maximum length will be ignored.

Note 2) Notes on CacheRoot directive

- If "On" is set for the ProxyRequests directive and the CacheRoot directive is not set, the proxy feature can be used but the cache feature cannot be used.
- **Solaris32/64 Linux32/64**
Set the following privileges for the directory in which the CacheRoot directive is set:
 - User: User set to the User directive
 - Group: Group set to the Group directive

Note 3) Notes on DocumentRoot directive

- In the initial state, the sample content is stored in the directory that is specified in DocumentRoot directive. Depending on the Web server operation, either delete unnecessary sample content, or change the directory that is specified in DocumentRoot directive.
- **Solaris32/64 Linux32/64**
The mount point to the NFS server can be specified, as long as it is always accessible while the Web server is running. To guarantee that, before starting the Web server, make sure that the NFS server has started normally, and while the Web server is running, do not perform operations that make the NFS server inaccessible (such as powering off the NFS server).

Note 4) Notes on ErrorDocument directive

- The error documents that can be specified in the ErrorDocument directive, and the status codes that can be notified to the client for that error document, are shown below. For details about the status codes, refer to the "Status Codes Reported from the Web Server" chapter of the Messages.

Error Document	Status Codes
Text message To specify the text message that is output, enclose the text message in double quotation marks ("").	300, 301, 302, 303, 400, 401, 403, 404, 405, 406, 407, 409, 410, 411, 413, 414, 415, 416, 417, 423, 424, 500, 501, 502, 503, 504, 506, 507
Inside URL To redirect to an internal URL, append a forward slash ("/") to the leading character and then specify the redirection destination as a relative path from the DocumentRoot directive.	204, 300, 301, 302, 303, 401, 403, 404, 405, 406, 409, 410, 411, 413(*), 415, 416, 423, 424, 500, 501(*), 502, 503, 504, 506, 507
Outside URL To redirect to an external URL, specify the redirect destination as a fully qualified URL.	204, 300, 301, 302, 303, 403, 404, 405, 406, 409, 410, 411, 413, 415, 416, 423, 424, 500, 501, 502, 503, 504, 506, 507

*) Internal redirection to static content can be specified, however internal redirection using CGI cannot be specified.

Note 5) Notes on ErrorLog directive

- "syslog" cannot be used in Interstage HTTP Server 2.2.
- If ErrorLog directive is set more than once for both the main host and virtual host, then the settings last defined for each will be the valid ones.

Note 6) Notes on FileETag directive

- The explanations for "Default" and "All" of the FileETag directive are incorrect. The correct explanations are shown below.

Mistake	Correct
Default: FileETag INode <u>MTime</u> <u>Size</u>	Default: FileETag INode <u>Size</u> <u>MTime</u>
All: All available fields will be used. This is equivalent to: FileETag INode <u>MTime</u> <u>Size</u>	All: All available fields will be used. This is equivalent to: FileETag INode <u>Size</u> <u>MTime</u>

Note 7) Notes on LimitInternalRecursion directive

- If the number of internal redirections or subrequests has exceeded the value set for the LimitInternalRecursion directive, a response is returned to the client with status code "500" (Internal Server Error).

Note 8) Notes on Listen directive

- IPv4-mapped addresses cannot be specified in the IP address specified in the Listen directive.
- **Windows32/64**
In Windows Server(R) 2003, IPv6 address link-local addresses cannot be specified in the IP address specified in the Listen directive. If a link-local address is specified, error message ahs00018 is output to the event log (application) and the web server will fail to start.
- **Linux32/64**
IPv6 address link-local addresses cannot be specified in the IP address specified in the Listen directive. If a link-local address is specified, error message ahs00018 is output to the event log (application) and the web server will fail to start.
- For port number, all the services on the system including applications must have different port numbers set.

Note 9) Notes on ListenBackLog directive

- The range specified for the maximum number of queues and default values set in the ListenBackLog directive will vary depending on the operating system. Each value is shown below.

	Range specified for the maximum number of queues	Default value
Windows32/64	1 - 200	ListenBacklog 200
Solaris32/64 Linux32/64	1 - 2147483647	ListenBacklog 511

- If there are more requests than the simultaneous number of client connections set by the MaxClients directive, the value that corresponds to the following conditions will be the maximum value for the number of queues waiting to be connected in the operating system.

	Condition	Maximum number of queues waiting for request processing
Windows32/64	None	Value set for the ListenBackLog directive
Solaris32/64 Linux32/64	Value set by this directive \leq Maximum number of TCP connections in standby (*1)	Value set for the ListenBackLog directive
	Value set by this directive $>$ Maximum number of TCP connections in standby (*1)	Maximum number of TCP connections in standby (*1)

*1 The maximum value for TCP connections in standby is set in the operating system. Execute the commands shown below to check this. For details on setting the TCP connections in standby and the command, refer to the operating system documents.

	Maximum number of TCP connections in standby	Command execution examples
Solaris32/64	tcp_conn_req_max_q	/usr/sbin/ndd /dev/tcp tcp_conn_req_max_q
Linux32/64	/proc/sys/net/core/somaxconn	/sbin/sysctl -n net.core.somaxconn

- If the connection request from the client exceeds the following value, this connection request will not be accepted and no status code will be returned.

Windows32/64

```
Simultaneous number of client connections + Maximum number of queues waiting for request processing + 1
```

Solaris32/64 Linux32/64

```
Simultaneous number of client connections + Maximum number of queues waiting for request processing + n
```

n: Value corresponding to the specifications of the operating system.

Note 10) Notes on MaxKeepAliveRequests directive

- When setting the maximum value for the server, it is recommended that you specify "0" for the number of requests. If a value of "1" or more is specified, the connection will be broken after the "specified number of requests + 1" requests have been processed.

Note 11) Notes on MaxRanges directive

- If the number of specified HTTP ranges set in the MaxRanges directive has exceeded the value set for the MaxRanges directive, the specified HTTP ranges will be invalid.

Note 12) Notes on MaxRequestsPerChild directive

Windows32/64

It is recommended that "0" always be specified as the number of HTTP requests set for the MaxRequestsPerChild directive. If a value other than "0" is specified, the environment definition file (httpd.conf) will be reloaded when the daemon process restarts. For this reason, if the environment definition is changed while the web server is running, this may reflect on the web server behavior at an unexpected time.

Note 13) Notes on SendBufferSize directive

- [Solaris32/64](#) [Linux32/64](#)

Check the TCP/IP send buffer size set for the operating system using the commands shown below. For details, refer to the document of the operating system.

	TCP/IP send buffer size	Command execution examples
Solaris32/64	tcp_xmit_hiwat	/usr/sbin/ndd /dev/tcp tcp_xmit_hiwat
Linux32/64	tcp_wmem	/sbin/sysctl -n net.ipv4.tcp_wmem [Display result] 4096 16384 131072 Note) The TCP/IP send buffer size is the middle value. The display result for the above will be "16384".

Note 14) Notes on ServerLimit directive

- Set the ServerLimit directive before the MaxClients directive.

Note 15) Notes on ServerName directive

- The IPv6 address cannot be specified in the ServerName directive.

Note 16) Notes on ThreadsPerChild directive

- [Windows32/64](#)

If there are more requests than specified with the value set for the ListenBackLog directive, they are saved in a queue on the web server and in the operating system. Use the ListenBacklog directive to set the number of queues in the operating system waiting to be connected.

- [Solaris32/64](#) [Linux32/64](#)

"1" must be set for linkage with the web server connector. The behavior of the web server cannot be guaranteed if a value other than "1" is set.

6.2 Directives provided in Interstage HTTP Server 2.2

The function of each directive provided in Interstage HTTP Server 2.2 is explained below.

Items which explain the directive

The items which explain the directive are shown below.

Name

Directive name

Synopsis

Directive format

Description

Functional overview of the directive

Context

Directive-set location indicated with one of the following keywords:

Global context

Setting used for action of the entire Web Server.

Virtual host

Setting which is available in the <VirtualHost> section and used for action of the virtual host.

Directory

Setting which is available in the <Directory>, <Location>, and <Files> sections and used for action in response to a request for a specified directory, URL, or file.

Default value

Value assumed when the directive is omitted. If a directive indicated with "None" is omitted, the directive function is disabled.

Initial value

Initial directive value

Module

Name of the module that implements the directive function. A directive with no module name indication is included in the basic module.

Note

Notes on the use of the directive

Examples

Directive example (included only for a directive which requires a complex setting).

6.2.1 ISSsoBusinessSystemName

Name

ISSsoBusinessSystemName

Synopsis

ISSsoBusinessSystemName *business-system-name*

Description

Embeds the Interstage Single Sign-on business server in the main host or virtual host.

Specify a maximum of 32 bytes for the business system name. Alphanumeric characters, and symbols except those shown below, can be used.

- Hyphen (-)
- Underscore (_)
- Left parenthesis ((
- Right parenthesis ())
- Left bracket ([
- Right bracket (])

Context

Global context, Virtual host

Default value

none

Examples

Embedding the Interstage Single Sign-on business server with the business system name "Business001" in the main host or virtual host

Windows32/64

```
LoadModule ssoatzihs22_module "C:/Interstage/F3FMssso/ssoatzag/lib/F3FMsssoatzihs22.dll"  
ISSsoBusinessSystemName Business001
```

Solaris32/64 **Linux32/64**

```
LoadModule ssoatzihs22_module "/opt/FJSVsssoaz/lib/ssoatzihs22.so"  
ISSsoBusinessSystemName Business001
```

6.2.2 SSLCertExpand

Name

SSLCertExpand

Synopsis

SSLCertExpand On|Off

Description

Specifies if the client certificate detailed item is set as the environment variable.

On

The client certificate detailed item is set as the environment variable.

Off

The client certificate detailed item is not set as the environment variable.

Context

Global context, Virtual host

Default value

For the main host:

```
SSLCertExpand On
```

For a virtual host:

```
SSLCertExpand (The value set for this main host directive)
```

Module

mod_ahs_ssl

6.2.3 SSLCertExpire

Name

SSLCertExpire

Synopsis

(1) When the Web server starts up, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire Startup day

(2) For the days/time specified while the Web server is running, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire Running days[...][:time]

(3) When the Web server starts up, and for the days/time specified while the Web server is running, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire All day days[...][:time]

(4) A warning message that notifies the number of days the certificate is still valid for is not output

SSLCertExpire None

Description

Set whether a warning message is output before the validity term of the site certificate and CA certificate expires. Additionally, if the warning message is output, set the timing for the output.

[Existence of output]

Startup

A warning message that notifies the number of days the certificate is still valid for is output using the day condition.

Running

A warning message that notifies the number of days the certificate is still valid for is output using the days (time) condition.

All

A warning message that notifies the number of days the certificate is still valid for is output using the day and days (time) conditions.

None

A warning message that notifies the number of days the certificate is still valid for is not output.

[Timing for the output]

day

When Startup/All are specified, specify how many days ahead of certificate expiry date a warning message is to be output in case Running/All are specified. The option must be specified as a number between 1 and 90 (unit: days). The timing for the output of the warning message is when the Web server starts up.

days

When Running/All are specified, specify how many days ahead of certificate expiry date a warning message is to be output in case Running/All are specified. The option must be specified as a number between 1 and 90 (unit: days). More than one day of the week can be specified. In this case, separate each day of the week using a comma (.). A maximum of 90 days can be specified. The timing for the output of the warning message is the days and time specified for days/time while the Web server is running.

time

When Running/All are specified, use the format shown below to specify the time at which the warning message is output. (If this is omitted, the format will be days and time left until the certificate's validity term expires.)

hhmmss (A numeric value between 000000 and 235959)

- hh: Hours (00-23)
- mm: Minutes (00-59)
- ss: seconds (00-59)

[Warning message that is output]

The warning messages shown below are output according to the output timing specified above.

- Warning message that notifies the number of days the site certificate is still valid for (ahs00536)
- Warning message that notifies the number of days the CA certificate is still valid for (ahs00537)

For details about the message, refer to the "[8.6.36 ahs00536](#)" and "[8.6.37 ahs00537](#)".

Context

Global context

Default value

```
SSLCertExpire All 14 90,60,30,14,7,6,5,4,3,2,1
```

Module

mod_ahs_ssl

6.2.4 SSLCertName

Name

SSLCertName

Synopsis

SSLCertName *nickname*

Description

Specifies the nickname of a site certificate registered in the certificate and CRL control environment, in up to 128 characters.

Only one SSLCertName directive can be defined for each host.

Context

Global context, Virtual host

Default value

none

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.5 SSLCipherSuite

Name

SSLCipherSuite

Synopsis

SSLCipherSuite *encryption-method*

Description

Specify the methods of encryption in descending order of priority. Use colons (:) as delimiters.

When the SSL protocol version "SSL2.0" is used (a value including 2 is specified in the [SSLVersion](#) directive), the following values can be specified.

Table 6.1 SSLVersion Directive Values if 2 or 2-3 is specified

Value	Explanation
RC4-MD5	SSL_TXT_RC4_128_WITH_MD5 (128 bit key)
RC2-MD5	SSL_TXT_RC2_128_CBC_WITH_MD5 (128 bit key)
DES-CBC3-MD5	SSL_TXT_DES_192_EDE3_CBC_WITH_MD5 (168 bit key)
DES-CBC-MD5	SSL_TXT_DES_64_CBC_WITH_MD5 (56 bit key)
EXP-RC4-MD5	SSL_TXT_RC4_128_EXPORT40_WITH_MD5 (40 bit key)
EXP-RC2-MD5	SSL_TXT_RC2_128_CBC_EXPORT40_WITH_MD5 (40 bit key)

When the SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) is used (a value including 3 or 3.1 is specified in the [SSLVersion](#) directive), the following values can be specified.

Table 6.2 SSLVersion Directive Values if 3 or 2-3 is specified

Value	Explanation
RSA-RC4-MD5	SSL_TXT_RSA_WITH_RC4_128_MD5 (128 bit key)
RSA-RC4-SHA	SSL_TXT_RSA_WITH_RC4_128_SHA (128 bit key)
RSA-3DES-SHA	SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA (168 bit key)
RSA-DES-SHA	SSL_TXT_RSA_WITH_DES_CBC_SHA (56 bit key)
RSA-EXPORT-RC4-MD5	SSL_TXT_RSA_EXPORT_WITH_RC4_40_MD5 (40 bit key)
RSA-EXPORT-RC2-MD5	SSL_TXT_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (40 bit key)
RSA-AES-128-SHA	SSL_TXT_RSA_WITH_AES_128_CBC_SHA (128 bit key)
RSA-AES-256-SHA	SSL_TXT_RSA_WITH_AES_256_CBC_SHA (256 bit key)
RSA-SC2000-128-SHA	SSL_TXT_RSA_WITH_SC2000_128_CBC_SHA (128 bit key)
RSA-SC2000-256-SHA	SSL_TXT_RSA_WITH_SC2000_256_CBC_SHA (256 bit key)
RSA-NULL-MD5	SSL_TXT_RSA_WITH_NULL_MD5
RSA-NULL-SHA	SSL_TXT_RSA_WITH_NULL_SHA

If 2-3 or 2-3.1 is specified for the [SSLVersion](#) directive, at least one value must be specified for each version.



The encryption types shown in the encryption method item ("SSL_TXT_XXX"):

- Public-key encryption method: RSA
- Private-key encryption method: DES, 3DES (triple DES), RC4, RC2, AES, SC2000 (NULL means no encryption.)
- Private-key processing mode: CBC, EDE (the numerical value shows the block length.)
- Hash key: SHA, MD5

Context

Global context, Virtual host

The following values are assumed according to the specified value for the [SSLVersion](#) directive. (In the following table, each encryption method is described on a new line for clarification.)

Table 6.3 Assumed Values of SSLVersion Directive if omitted

Value of the SSLVersion directive	Default value of this directive
2	DES-CBC3-MD5: RC4-MD5: RC2-MD5: DES-CBC-MD5: EXP-RC2-MD5: EXP-RC4-MD5
3 3.1 3-3.1	RSA-SC2000-256-SHA: RSA-AES-256-SHA: RSA-SC2000-128-SHA: RSA-AES-128-SHA: RSA-3DES-SHA: RSA-RC4-MD5: RSA-RC4-SHA: RSA-DES-SHA: RSA-EXPORT-RC4-MD5: RSA-EXPORT-RC2-MD5
2-3 2-3.1	DES-CBC3-MD5: RC4-MD5: RC2-MD5: DES-CBC-MD5: EXP-RC2-MD5: EXP-RC4-MD5: RSA-SC2000-256-SHA: RSA-AES-256-SHA: RSA-SC2000-128-SHA: RSA-AES-128-SHA: RSA-3DES-SHA: RSA-RC4-MD5: RSA-RC4-SHA: RSA-DES-SHA: RSA-EXPORT-RC4-MD5: RSA-EXPORT-RC2-MD5

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.6 SSLClCACertName

Name

SSLClCACertName

Synopsis

SSLClCACertName *nickname*

Description

Specifies the nickname of the CA certificate for confirming a client certificate, in up to 128 characters. This directive is used to select a specific certificate from client CA certificates registered in the operation control directory. The directive is enabled when SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) is used.

Multiple SSLClCACertName directives can be defined for each host and each definition is enabled only for the corresponding host.

Context

Global context, Virtual host

Default value

SSLClCACertName (The nicknames of all client CA certificates registered in the operation control directory are specified.)
--

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.7 SSLConfName

Name

SSLConfName

Synopsis

SSLConfName *SSL-definition*

Description

Configures the Interstage certificate environment SSL definition that was built in the Interstage Management Console.

Specify [Configuration Name] of Interstage management console [Security] > [SSL] > [Create an SSL Configuration] tab for the SSL definition.

Context

Global context, Virtual host

Default value

none

Module

mod_ahs_ssl

Note

- Operations can use the SSL of the certificate/key management environment built using the SMEE command or the Interstage certificate environment SSL; both cannot be used together. If the certificate/key management environment SSL definition built using the SMEE command has been configured, delete all SSL definitions and then configure this directive.
- This directive cannot be configured in conjunction with the directives shown below. If these directives are configured at the same time, the configuration for this directive will be invalid.
 - [SSLCertName](#)
 - [SSLCipherSuite](#)
 - [SSLCICACertName](#)
 - [SSEnvDir](#)
 - [SSEExec](#)
 - [SSLSlotDir](#)
 - [SSLTokenLabel](#)
 - [SSLUserPINFile](#)
 - [SSLVerifyClient](#)
 - [SSLVersion](#)

6.2.8 SSEnvDir

Name

SSEnvDir

Synopsis

SSEnvDir *operation-control-directory-name*

Description

Specifies the operation control directory used for SSL along with the absolute path.

Only one SSEnvDir directive can be defined for each host.

Context

Global context, Virtual host

Default value

none

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.9 SSLExec

Name

SSLExec

Synopsis

SSLExec On|Off

Description

Specifies whether SSL is used.

Only one SSLExec directive can be defined for each host.

On

SSL is used.

Off

SSL is not used.

Context

Global context, Virtual host

Default value

SSLExec Off

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.10 SSLHandshakeTimeout

Name

SSLHandshakeTimeout

Synopsis

SSLHandshakeTimeout *seconds*

Description

Sets the maximum wait time (in seconds) after a data packet is sent/received to/from the client in SSL connection establishment processing. A number from 0 to 2147483647 can be specified for the wait time. If the packet cannot be received even though the specified wait time is exceeded, the connection is closed. If "0" is specified, the wait time is unlimited.

Normally, this is set so that the time taken for SSL connection establishment processing can be tuned.

Context

Global context

Default value

```
SSLHandshakeTimeout (The value set for the Timeout directive)
```

Module

mod_ahs_ssl

6.2.11 SSLLIBMultiSession

Name

SSLLIBMultiSession

Synopsis

SSLLIBMultiSession concurrency

Description

Specifies the concurrency for the initial startup of the encrypted library. A number from 1 to 256 can be specified for the concurrency. If the value that is set is increased, communication processing for multiple connections immediately after startup becomes faster. If the value that is set is increased, however, note that the start processing time also increases.

Context

Global context

Default value

```
SSLLIBMultiSession 50
```

Module

mod_ahs_ssl

Note

- The value that is set for this directive is extended automatically according to the number of requests, so in normal cases there is no need for it to be set.
- If one of the methods shown below is used to restart the web server after the value that was configured for this directive is changed, the changes to the value that was configured will be invalid. To enable the changes to the value that was configured for this directive, stop the web server and then restart it.
 - The restart option or graceful option is specified in the apachectl command, and the command is then executed
 - The restart parameter or graceful parameter is specified in the -k option of the httpd command, and the command is then executed

6.2.12 SSLMaxSession

Name

SSLMaxSession

Synopsis

Number of SSLMaxSession requests

Description

Specifies the maximum number of requests used to retain SSL session information. A number from 1 to 65535 can be specified for the number of requests. Once SSL communication is performed, and SSL session information is retained on the server machine, it is possible to improve the request forwarding efficiency.

This directive is enabled if "SSL 3.0" or more is set for the SSL protocol version in the [SSLVersion](#) directive.

Context

Global context

Default value

```
SSLMaxSession 100
```

Module

mod_ahs_ssl

Note

- Approximately 4 kilobytes of virtual memory are used up for each increase of 1 in the value that is set for the number of requests. When tuning the application status, take care not to set a value that is too great.
- If one of the methods shown below is used to restart the web server after the value that was configured for this directive is changed, the changes to the value that was configured will be invalid. To enable the changes to the value that was configured for this directive, stop the web server and then restart it.
 - The restart option or graceful option is specified in the apachectl command, and the command is then executed
 - The restart parameter or graceful parameter is specified in the -k option of the httpd command, and the command is then executed

6.2.13 SSLNotifyVers

Name

SSLNotifyVers

Synopsis

```
SSLNotifyVers On|Off
```

Description

Specifies whether an SSL-related environment variable is set.

On

SSL-related information is set as the environment variable.

Off

SSL-related information is set as the environment variable. However, the HTTPS environment variable is set.

Context

Global context, Virtual host

Default value

For the main host:

```
SSLNotifyVers On
```

For a virtual host:

```
SSLNotifyVers (The value set for this main host directive)
```

Module

mod_ahs_ssl

6.2.14 SSLSlotDir

Name

SSLSlotDir

Synopsis

SSLSlotDir *slot-information-directory*

Description

Specifies the slot information directory for the private key control environment along with the absolute path.

Only one SSLSlotDir directive can be defined for the basic area of the environment definition file (httpd.conf).

Context

Global context

Default value

none

Module

mod_ahs_ssl

Note

- This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.
- If one of the methods shown below is used to restart the web server after the value that was configured for this directive is changed, the changes to the value that was configured will be invalid. To enable the changes to the value that was configured for this directive, stop the web server and then restart it.
 - The restart option or graceful option is specified in the apachectl command, and the command is then executed
 - The restart parameter or graceful parameter is specified in the -k option of the httpd command, and the command is then executed

6.2.15 SSLTokenLabel

Name

SSLTokenLabel

Synopsis

SSLTokenLabel *token-label*

Description

Specifies the token label of the token in which the private key of the server is registered, in up to 32 characters.

Only one SSLTokenLabel directive can be defined for the basic area of the environment definition file (httpd.conf).

Context

Global context

Default value

none

Module

mod_ahs_ssl

Note

- This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.
- If one of the methods shown below is used to restart the web server after the value that was configured for this directive is changed, the changes to the value that was configured will be invalid. To enable the changes to the value that was configured for this directive, stop the web server and then restart it.
 - The restart option or graceful option is specified in the apachectl command, and the command is then executed
 - The restart parameter or graceful parameter is specified in the -k option of the httpd command, and the command is then executed

6.2.16 SSLUserPINFile

Name

SSLUserPINFile

Synopsis

SSLUserPINFile *user-PIN-file-name*

Description

Specifies a user PIN file along with the absolute path.

Only one SSLUserPINFile directive can be defined for the basic area of the environment definition file (httpd.conf).

For information on creating a user PIN file, refer to "[7.7 ihsregistupin](#)".

Context

Global context

Default value

none

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.17 SSLVerifyClient

Name

SSLVerifyClient

Synopsis

SSLVerifyClient none|optional|require

Description

Specifies the level of client certification when using SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0).

Only one SSLVerifyClient directive can be defined for each host.

none

Does not verify a client certificate.

optional

Verifies a client certificate.

When a client does not provide the client certificate, the processing continues.

require

Verifies a client certificate.

When a client does not provide the client certificate, an error occurs.

When "2" is specified with the [SSLVersion](#) directive, this directive must be omitted or set to "none".

Context

Global context, Virtual host

Default value

One of the following values is specified according to the value specified with the SSLVersion directory.

Table 6.4 Assumed Values of SSLVersion Directive if omitted

Value of the SSLVersion directive	Default value of this directive
2	none
3	optional
3.1	optional
2-3	optional
2-3.1	optional
3-3.1	optional

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.18 SSLVersion

Name

SSLVersion

Synopsis

SSLVersion 2|3|3.1|2-3|2-3.1|3-3.1

Description

Specifies the version of SSL protocol to be used.

Only one SSLVersion directive can be defined for each host.

2

Uses SSL protocol version "SSL2.0".

3

Uses SSL protocol version "SSL3.0".

3.1

Uses SSL protocol version "SSL3.1" (TLS 1.0).

2-3

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL2.0"
- SSL protocol version "SSL3.0"

2-3.1

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL2.0"
- SSL protocol version "SSL3.0"
- SSL protocol version "SSL3.1" (TLS 1.0)

3-3.1

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL3.0"
- SSL protocol version "SSL3.1" (TLS 1.0)

Context

Global context, Virtual host

Default value

```
SSLVersion 3-3.1
```

Module

mod_ahs_ssl

Note

This directive cannot be specified if the [SSLConfName](#) directive is specified. If it is, the settings for this directive are invalid.

6.2.19 Trace

Name

Trace

Synopsis

Trace On|Off

Description

Configures the trace information collection setting.

On

The trace information is collected in the trace file. The trace file configuration is set in the [TraceLog](#) directive.

Off

The trace information is not collected in the trace file.

Context

Global context

Default value

Trace On

Note

- If this directive is configured more than once, the most recent configuration will be used.
- It is recommended that "On" always be configured for this directive, so that the trace information is collected. If no trace information is output, it may prove to be an obstacle to investigations when a problem occurs.

6.2.20 TraceLog

Name

TraceLog

Synopsis

Windows32/64
TraceLog "*||ahsrlog-command-execution-statement*"*trace-file-name*

Solaris32/64 **Linux32/64**
TraceLog "*ahsrlog-command-execution-statement*"*trace-file-name*

Description

Creates the trace file and outputs the following information:

- Web client input/output information
- Plugin module input/output information

||ahsrlog-command-execution-statement **Windows32/64**
ahsrlog-command-execution-statement **Solaris32/64** **Linux32/64**

Specifies the *ahsrlog* command execution statement.

For details about the *ahsrlog* command execution statement, refer to the "[7.3 ahsrlog](#)".

trace-file-name

Specifies the name of the file to which trace information are to be output.

Specify the absolute path to the trace file. If the specified path does not begin with a slash "/", it is assumed to be the relative path from the `ServerRoot` directive. Specify the name of an already existing directory.

Context

Global context

Default value

Windows32/64

```
TraceLog logs/trace.log
```

Solaris32/64 Linux32/64

```
TraceLog logs/trace_log
```

Initial value

Windows32/64

```
TraceLog " ||C:/Interstage/F3FMahs/bin/ahsrlog.exe -s C:/Interstage/F3FMahs/logs/tracelog 2 5"
```

Solaris32/64 Linux32/64

```
TraceLog " | /opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/tracelog 2 5"
```

Note

- This directive is enabled when the configuration is for the trace information to be collected ("On" has been configured in the [Trace](#) directive). If you do not want the trace information to be output, configure the setting to "Off" in the [Trace](#) directive.
- If this directive is configured more than once, the most recent configuration will be used.

Chapter 7 Commands

This chapter provides the Interstage HTTP Server 2.2 operation commands.



See

Refer to the "Apache HTTP Server Version 2.2 Documentation" for details on the Apache HTTP Server Version 2.2.22 offer command. This documentation is contained in "apache\httpd-docs-2.2.22.en.zip". Extract this file, open folder "httpd-docs-2.2.22.en", and then open index.html.

Supported commands

The following table describes the commands supported by each product.

Command	Outline	Directory (default installation path)	Remarks
ahsbackup	Backup and export of resources for Interstage HTTP Server 2.2	Windows32/64 C:\Interstage\F3FMahs\bin	Commands provided with Interstage HTTP Server 2.2
ahsrestore	Restore and import of resources for Interstage HTTP Server 2.2	Solaris32/64 Linux32/64 /opt/FJSVahs/bin	
ahslog	Rotate log files		
ihsregistupin	Register user PINs		
htpasswd	Edit password files for user authentication		
httpd	Start and stop the web server, and register and remove the web server services		Commands provided with Apache HTTP Server Version 2.2.22
apachectl Solaris32/64 Linux32/64	Start and stop the web server	- For the default web server /opt/FJSVahs/bin - For multiple web server operation <directory containing the web server resources>/bin	



Note

- Some commands have the same name in Interstage HTTP Server and Interstage HTTP Server 2.2. To distinguish between Interstage HTTP Server and Interstage HTTP Server 2.2 commands, it is necessary to specify the absolute path to execute the Interstage HTTP Server 2.2 command.
- When entering commands, use a space as a delimiter to separate the command name from its parameters and to separate parameters from each other. To specify a string containing spaces in a command parameter, specify the relevant parameter inside double quotation marks, as shown in the following example:

```
C:\Interstage\F3FMahs\bin\httpd.exe -k start -n "Interstage HTTP Server 2.2"
```



Point

Method to indicate the commands

Symbols below are used to explain the command synopsis.

- Square brackets []

This indicates that the items described in the square brackets can be omitted. Only one item can be selected if more than one item is described.

- Curly brackets { }

This indicates that one item must be selected and specified from multiple items described in the curly brackets.

- Option symbol |

This symbol separates multiple items to choose from.

- Multiple selection symbol ,

This symbol indicates that more than one item can be selected from the multiple items specified within the square brackets or curly brackets.

- Repeat symbol ...

This indicates that the item immediately before this symbol can be repeated any number of times.

7.1 ahsbackup

Name

ahsbackup

Backup and export of resources for Interstage HTTP Server 2.2

Synopsis

```
ahsbackup -d directory [-t pass|all]
```

Description

This command backs up and exports resources files used by Interstage HTTP Server 2.2.

The options and parameters of this command are as follows:

-d directory

Windows32/64

Specify the storage directory name of the Interstage HTTP Server 2.2 resources for backup/export (the name can be up to 256 bytes).

Backups of the Interstage HTTP Server resources are saved at the level below the specified directory in the "AHS" directory.

If this directory already exists, delete it before using the command. Also delete the directory if the backup and export terminates abnormally.

Solaris32/64 Linux32/64

Specify the storage directory name (full pathname) of the Interstage HTTP Server 2.2 resources for backup/export (the name can be up to 256 bytes).

Backups of the Interstage HTTP Server resources are saved at the level below the specified directory in the "FJSVahs" directory:

If this directory already exists, delete it before using the command. Also delete the directory if the backup and export terminates abnormally.

-t pass|all

Specify the backup/export target resources from those shown in the table below. Select the resources according to the environment that is used.

Backup/export target resources		Details of backed up resources (default installation path)	-t option is specified		
			-t option is omitted	-t pass	-t all
Resources on all web servers	Web server list file	Windows32/64 C:\Interstage\F3FMahs\etc\servers.conf Solaris32/64 Linux32/64 /etc/opt/FJSVahs/etc/servers.conf	OK	OK	OK
Resources on each web server	Environment definition information	Environment definition file (httpd.conf) (*1) and Files and directories specified in the following directives of the environment definition file (httpd.conf) (*1) - Include - MIMEMagicFile - TypesConfig	OK	OK	OK
	Password file (If performing user authentication)	Files specified in the following directives of the environment definition file (httpd.conf) (*1) - AuthGroupFile - AuthUserFile - AuthDBMGroupFile - AuthDBMUserFile	No	OK	OK
	Contents	Files and directories specified in the following directives of the environment definition file (httpd.conf) (*1) - DocumentRoot - Alias - ScriptAlias	No	No	OK
	Web server resources	Directories specified in the ServerRoot directive of the environment definition file (httpd.conf) (*2)	OK	OK	OK

OK: Backup/export is performed.

No: Backup/export is not performed.

*1) All the environment definition files (httpd.conf) specified in the web server list file (servers.conf) are backup targets.

*2) Environment definition files (httpd.conf) other than web servers specified in the web server list file (servers.conf), are backup targets.

Notes

- Execute this command with administrator authority.
- Execute this command when all web servers have been stopped.

- For the contents that do not belong to the directory specified by the DocumentRoot/Alias/ScriptAlias directive and CGI resources, separately back up and export the corresponding files.
- All files including those starting with a period (.) must be the target for operations when performing compressions and copies on backup and import resources.
- If a path that contains a wildcard is specified in the Include directive, it will not be a backup target.
- **Solaris32/64** **Linux32/64**
The root directory (/) cannot be specified as the storage directory of the Interstage HTTP Server resources, which is specified by the -d option.
- **Solaris32/64** **Linux32/64**
If a symbolic link is specified in the directive, the backup/export target will be the directory/file at the link destination. Note that backup/export resources for which a symbolic link has been specified will be restored as an actual directory or file.
- If the SSL of the Interstage Certificate Environment established with the Interstage Management Console is used, the Interstage Certificate Environment resources need to be backed up and exported.
- If the SSL of the certificate/key management environment established with the SMEE command is used, back up and export the following resources, each of which is specified by the corresponding directive in the environment definition file (httpd.conf):
 - Slot information directory (directory specified in SSLSlotDir directive)
 - Operation control directory (directory specified in SLEnvDir directive)
 - User PIN control file (directory specified in SSLUserPINFile directive)

Example

Windows32/64

The Interstage HTTP Server 2.2 resources are backed up to the "X:\Backup\AHS" directory.

```
C:\Interstage\F3FMahs\bin\ahsbackup.exe -d X:\Backup -t all
```

Solaris32/64 **Linux32/64**

The Interstage HTTP Server 2.2 resources are backed up to the "/backup/FJSVahs" directory.

```
/opt/FJSVahs/bin/ahsbackup -d /backup -t all
```

7.2 ahsrestore

Name

ahsrestore

Restore and import of resources for Interstage HTTP Server 2.2

Synopsis

```
ahsrestore -d directory [-t pass|all] [-h host_table]
```

Description

This command restores and imports the Interstage HTTP Server resources backed up/exported by the [ahsbackup](#) command.

The options and parameters of this command are as follows:

-d directory

Windows32/64

Specify the storage directory name of the Interstage HTTP Server resources (the name can be up to 256 bytes). Specify the directory name specified by the [ahsbackup](#) command.

Solaris32/64 Linux32/64

Specify the storage directory name (full pathname) of the Interstage HTTP Server resources (the name can be up to 256 bytes). Specify the directory name specified by the [ahsbackup](#) command.

-t pass|all

Specify the restore/import target resources. This argument depends on the options specified when the [ahsbackup](#) command is executed. For details on the restore/import target resources, refer to the [ahsbackup](#) command.

What is specified when the ihsbackup command is executed		
-t option is omitted	-t pass	-t all
-t option is omitted	-t pass	-t all
	-t option is omitted	-t pass
		-t option is omitted

-h host_table

This option allows you to change host names and IP addresses at the time of import. By specifying the full path to a file in which the new and old host names and IP addresses are written, names and addresses can automatically be converted at the time of import.

The file with the new host names and IP addresses should be written as follows:

- A hash mark (#) is placed at the beginning of each comment line.
- Halfwidth space characters and tab characters are ignored.

```
### Host IP conversion table ###
# IP address conversion definition
(IP address before conversion) > (IP address after conversion)
:
# Host name conversion definition
(Host name before conversion) > (Host name after conversion)
:
```

 **Example**

When the host name and IP address are to be converted as follows:

Before conversion	After conversion
IP address: "192.168.0.1"	IP address: "192.168.0.3"
IP address: "192.168.0.2"	IP address: "192.168.0.4"
Host name: "www.fujitsu.com"	Host name: "www.interstage.com"
Host name: "host1.fujitsu.com"	Host name: "host2.fujitsu.com"

```

### Host IP conversion table ###

# IP address conversion definition
192.168.0.1 > 192.168.0.3
192.168.0.2 > 192.168.0.4

# Host name conversion definition
www.fujitsu.com > www.interstage.com
host1.fujitsu.com > host2.fujitsu.com

```

Notes

- Execute this command with administrator authority.
 - Stop all web servers before restoring.
 - If the restore and import destinations contain files, those files will be overwritten.
 - The system where restore and import is performed needs to have the same disk configuration as the system where backup and export has been performed.
 - The host name/IP address converted with the -h option are specified in the directives below.
 - Listen
 - ServerName
 - VirtualHost
 - NameVirtualHost
 - For the contents that do not belong to the directory specified by the DocumentRoot/Alias/ScriptAlias directive and CGI resources, separately restore and import the corresponding files.
 - When restoring or importing resources that have been backed up or exported, ensure that one of the following conditions applies:
 - Only the default web server exists
 - All the following match in the backup, import source and restore, and import destination operating environments:
 - Number of web servers
 - Name of each web server (*1)
 - Path of the environment definition file for each web server (*1) (*2)
 - *1) **Solaris32/64** **Linux32/64**
 - The uppercase and lowercase letters must match.
 - *2) **Windows32/64**
 - The environment definition file (httpd.conf) paths (including, 8.3 formats (short names)) set in the web server list file (servers.conf) must also match.
- Windows32/64**
- In either of the above conditions, it is also necessary that the path specified in the environment definition file when registering the service is the same for backups, export source and restores, and import destination environment services with the same service name.
- Interstage HTTP Server resources that have been backed up or exported with the ihsbackup command cannot be restored or imported.
 - If the SSL of the Interstage Certificate Environment established with the Interstage Management Console is used, the Interstage Certificate Environment resources that have been backed up and need to be restored and imported.
 - If the SSL of the certificate/key management environment established with the SMEE command is used, restore and import the following resources, to the paths specified with the corresponding directives of the environment definition file (httpd.conf):
 - Slot information directory (directory specified in SSLSlotDir directive)
 - Operation control directory (directory specified in SLEnvDir directive)

- User PIN control file (directory specified in SSLUserPINFile directive)

- **Solaris32/64** **Linux32/64**

When performing restores and imports, the web server list file (servers.conf) uses the same file attributes as those of the restore/import destination operation environment (access privileges, file owners, or groups that file owners belong to). If the file attributes of the backup/export source and restore/import destination operation environment are different, change the backup/export source file attributes as required.

Examples

Windows32/64

Backup resources of Interstage HTTP Server 2.2 are restored.

```
C:\Interstage\F3FMahs\bin\ahsrestore.exe -d X:\Backup -t all
```

Solaris32/64 **Linux32/64**

Backup resources of the Interstage HTTP Server 2.2 are restored.

```
/opt/FJJSVahs/bin/ahsrestore -d /backup -t all
```

7.3 ahsrlog

Name

ahsrlog

Rotate log files

Synopsis

1. Rotating through log files in units of time

```
ahsrlog -T logfile time[...] count [-l maxsize] [-m mode] [-r]
```

2. Rotating through log files in units of date/time

```
ahsrlog -C logfile date[...] count [-t time] [-l maxsize] [-m mode] [-r]
```

3. Rotating through log files in units of days of week/time

```
ahsrlog -W logfile week[...] count [-t time] [-l maxsize] [-m mode] [-r]
```

4. Rotating through log files in units of days

```
ahsrlog -d logfile days count [-m mode]
```

5. Rotating through log files in units of file sizes

```
ahsrlog -s logfile size count [-m mode]
```

Description

This command specifies whether a log file to which access log, error log, or trace log information is output is created in units of file size or units of days.

This command is used to specify the ErrorLog directive parameter, CustomLog directive parameter, TraceLog directive parameter, and TransferLog directive parameter in the environment definition file (httpd.conf).

The options and parameters of this command are as follows:

-T

Rotating through log files in units of time and file size is performed according to the following timing:

- At time specified for 'time'.
- When the file size specified for the -l option is exceeded once the log file is updated.
- When the -r option is specified, the log file (*filename-prefix*) specified for 'logfile' already exists and the file size is 1 byte or more when the web server starts.

If no log is output, a 0-byte log file is created at the time specified for 'time'.

-C

Rotating through log files in units of date and file size is performed according to the following timing:

- At date specified for 'date' and 'time' specified for the -t option.
- When the file size specified for the -l option is exceeded once the log file is updated.
- When the -r option is specified, the log file (*filename-prefix*) specified for 'logfile' already exists and the file size is 1 byte or more when the web server starts.

If no log is output, a 0-byte log file is created at the time specified for the -t option.

-W

Rotating through log files in units of days of week and file size is performed according to the following timing:

- At days of week specified for 'week' and 'time' specified for the -t option.
- When the file size specified for the -l option is exceeded once the log file is updated.
- When the -r option is specified, the log file (*filename-prefix*) specified for 'logfile' already exists and the file size is 1 byte or more when the web server starts.

If no log is output, a 0-byte log file is created at the time specified for the -t option.

-d

Rotating through log files in units of number of days is performed according to the following timing:

- When the next log is output after number of days specified for 'days' starting from 0:00 on the web server startup date * 24 hours.

Rotating through log files is also performed according to the following conditions, but there are no changes at the timings mentioned above.

- If the following file size upper limit is exceeded when the log file is updated.

Windows32/64

2G bytes

Solaris32/64 Linux32/64

If the file size set by the *ulimit* command (Bourne shell type) or the *limit* command (C shell type) is at least 2G bytes, the file size is 2G bytes. If the file size set in the *ulimit* command or *limit* command is smaller, then that size is used.

- When the first log is output after the web server starts, the log file (*filename-prefix*) specified for 'logfile' already exists and "Date modified" for that log file is different to "Date started up" for the web server.

-S

Rotating through log files in units of file size is performed according to the following timing:

- When the size specified for the *size* parameter is exceeded once the log file is updated.

logfile

Specifies the directory where the log file is stored and the prefix for the log file name (the name can be up to 192 bytes).

An existing directory name is specified using the absolute path.

The log file is output in the following format:

- Latest file: *filename-prefix*
- Rotated file: *filename-prefix.N*

N: Serial number

N is a serial number beginning at 0. The serial numbers are assigned in order from the latest file, whose serial number is ".0". The serial number of the Nth file is ".(N-1)".

time[,...]

Specify the time at which rotating through log files is performed using the format below. Up to 24 times can be specified, each separated by a comma (,).

- Format: "hhmm" (numeric value from 0000 to 2359)
 - hh: hours (00 to 23)
 - mm: minutes (00 to 59)

date[,...]

Specify the date on which rotating through log files is performed as a numeric value between 1 and 31. Up to 31 dates can be specified, each separated by a comma (,).

week[,...]

Specify the day of the week on which rotating through log files is performed as one of the following character strings. Up to 7 days of the week can be specified, each separated by a comma (,). The values are not case-sensitive.

- Sunday: "Sun"
- Monday: "Mon"
- Tuesday: "Tue"
- Wednesday: "Wed"
- Thursday: "Thu"
- Friday: "Fri"
- Saturday: "Sat"

days

Specify the interval at which rotating through log files is performed as number of days between 1 and 365.

size

Specify the maximum log file size in MB as a numeric value between 1 and the following value.

 Windows32/64
2047

Solaris32/64 **Linux32/64**

If the file size set by the *ulimit* command (Bourne shell type) or the *limit* command (C shell type) is at least 2047M bytes, the file size is 2047M bytes. If the file size set in the *ulimit* command or *limit* command is small, that file size is used.

count

Specify the maximum number of log files as a number between 0 and 999.

If the file count has reached the upper limit, then the oldest log file is deleted and a new one created according to the option specified for determining rotating through log files.

If "0" or "1" was specified, the log file (*filename-prefix*) specified for 'logfile' is used.

-t time

Specify the time at which rotating through log files is performed using the format below.

- Format: "hhmm" (numeric value from 0000 to 2359)

- hh: hours (00 to 23)

- mm: minutes (00 to 59)

If this option is omitted, then the log files will be rotated through at "0000" (00hh 00mm).

-l maxsize

Specify the file size file in MB that will cause the log file to rotate. Specify a numeric value between 1 and the following value. If the file size exceeds this value when the log file is updated, then rotating will be performed.

Windows32/64

2047

Solaris32/64 **Linux32/64**

If the file size set by the *ulimit* command (Bourne shell type) or the *limit* command (C shell type) is at least 2047M bytes, the file size is 2047M bytes. If the file size set in the *ulimit* command or *limit* command is small, that file size is used.

If this option is omitted, the maximum log file size will be the following numerical value:

Windows32/64

2G bytes

Solaris32/64 **Linux32/64**

If the file size set by the *ulimit* command (Bourne shell type) or the *limit* command (C shell type) is at least 2G bytes, the file size is 2G bytes. If the file size set in the *ulimit* command or *limit* command is small, that file size is used.

-m mode **Solaris32/64** **Linux32/64**

Specify the log file access authority. The values in the table below can be specified for "mode".

If this option is omitted, then the log file access authority is set to "644", which means that the administrator will have read and write authority, whereas groups and general users will only have read authority.

Mode	Administrator authorities		Group authorities		General Users authorities	
	Read	Write	Read	Write	Read	Write
600	Yes	Yes	No	No	No	No
640	Yes	Yes	Yes	No	No	No
644 (omitted)	Yes	Yes	Yes	No	Yes	No
660	Yes	Yes	Yes	Yes	No	No
664	Yes	Yes	Yes	Yes	Yes	No

Mode	Administrator authorities		Group authorities		General Users authorities	
	Read	Write	Read	Write	Read	Write
666	Yes	Yes	Yes	Yes	Yes	Yes

Yes: There is access authority.

No: There is no access authority.

-r

When the log file (*filename-prefix*) specified for 'logfile' already exists and the file size is 1 byte or more, rotating through log files is performed when the web server starts.

If this option is omitted, rotating through log files will not be performed when the web server starts.

Notes

- Specify the options and parameters for this command in the order shown in "Synopsis".
- If the web server or operating system is restarted periodically, then log file rotation may not be performed.
If the following cases apply, specify the -r option to start the web server.
 - If the web server or operating system was not running when the -T option was specified and at the time specified for 'time'
 - If the web server or operating system was not running when the -C option was specified and at the time specified for the -t option of the date specified for 'date'
 - If the web server or operating system was not running when the -W option was specified and at the time specified for the -t option of the day of the week specified for 'week'
- Do not copy/move/delete/edit the log file (*filename-prefix*) specified for 'logfile'.
- Do not specify the same log file (*filename-prefix*) in the main host and virtual host, or in a different directory.
- If multiple web servers are running, do not specify the same log file (*filename-prefix*) as another web server.
- For months not containing 31 days, rotating through log files will not be performed on the 31st, even if "31" is specified for the -C option. If you want rotating through log files to be performed at the end of the month, investigate setting rotating through log files to be performed at 00hh 00mm on the 1st.
- The timestamp of the old log file is the date when the last log file was written.
- For details on the *ulimit* command (Bourne shell type) and *limit* command (C shell type), refer to each OS document.

Examples

Windows32/64

- When access log file rotation is performed in units of time according to the conditions below:
 - Rotation time: 09hh 00mm, 17hh 00mm
 - File Name: C:\Interstage\F3FMahs\logs\accesslog
 - File count upper limit: 5

```
CustomLog "|\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -T \\"C:/Interstage/F3FMahs/logs/accesslog
\" 0900,1700 5" ahs-analysis
```

- When access log file rotation is performed in units of date/time according to the conditions below:
 - Dates: 1st, 11th, 21st of every month

- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "|\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -C \\"C:/Interstage/F3FMahs/logs/accesslog
\" 1,11,21 5" ahs-analysis
```

- When access log file rotation is performed in units of days of the week/time according to the conditions below:

- Days of Week: Monday and Saturday of every week
- Rotation time: 00hh 00mm
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "|\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -W \\"C:/Interstage/F3FMahs/logs/accesslog
\" Mon,Sat 5" ahs-analysis
```

- When access log file rotation is performed in units of number of days according to the conditions below:

- Number of days: 1 day
- Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "|\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -d \\"C:/Interstage/F3FMahs/logs/accesslog
\" 1 5" ahs-analysis
```

- When access log file rotation is performed in units of file size according to the conditions below:

- File Size: 1M byte
- File Name: C:\Interstage\F3FMahs\logs\accesslog
- File count upper limit: 5

```
CustomLog "|\\"C:/Interstage/F3FMahs/bin/ahsrlog.exe\" -s \\"C:/Interstage/F3FMahs/logs/accesslog
\" 1 5" ahs-analysis
```

Solaris32/64 **Linux32/64**

- When access log file rotation is performed in units of time according to the conditions below:

- Rotation time: 09hh 00mm, 17hh 00mm
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -T /opt/FJSVahs/logs/accesslog 0900,1700 5" ahs-analysis
```

- When access log file rotation is performed in units of date/time according to the conditions below:

- Dates: 1st, 11th, 21st of every month
- Rotation time: 00hh 00mm
- File Name: /var/opt/FJSVahs/logs/accesslog
- File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -C /opt/FJSVahs/logs/accesslog 1,11,21 5" ahs-analysis
```

- When access log file rotation is performed in units of days of the week/time according to the conditions below:
 - Days of Week: Monday and Saturday of every week
 - Rotation time: 00hh 00mm
 - File Name: /var/opt/FJSVahs/logs/accesslog
 - File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -W /opt/FJSVahs/logs/accesslog Mon,Sat 5" ahs-analysis
```

- When access log file rotation is performed in units of number of days according to the conditions below:
 - Number of days: 1 day
 - Rotation time: When the next log is output after "number of days (1 day) starting from 0:00 on the web server startup date * 24 hours"
 - File Name: /var/opt/FJSVahs/logs/accesslog
 - File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -d /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis
```

- When access log file rotation is performed in units of file size according to the conditions below:
 - File Size: 1M byte
 - File Name: /var/opt/FJSVahs/logs/accesslog
 - File count upper limit: 5

```
CustomLog "|/opt/FJSVahs/bin/ahsrlog -s /opt/FJSVahs/logs/accesslog 1 5" ahs-analysis
```

7.4 apachectl

Name

apachectl

Start and stop the web server

Synopsis

Solaris32/64 **Linux32/64**

```
apachectl start | stop
```

Description

This command starts and stops the web server.

The options of this command are as follows:

start

Starts the web server.

stop

Stops the web server.

Notes

- Execute this command with administrator authority.
- Apart from the above options, the options for this command in Apache HTTP Server Version 2.2 can also be used. For details about these options, refer to the "Apache HTTP Server Version 2.2 Documentation". However, the "restart" option and the "graceful" option cannot be used when using the following features:
 - Web Server Connector (for Interstage HTTP Server 2.2)
 - Interstage Single Sign-on (Business server)

Examples

Starts the default web server.

```
/opt/FJSVahs/bin/apachectl start
```

Stops the default web server.

```
/opt/FJSVahs/bin/apachectl stop
```

Starts the web server of multiple web server operation.

```
<directory containing the web server resources>/bin/apachectl start
```

Stops the web server of multiple web server operation.

```
<directory containing the web server resources>/bin/apachectl stop
```

7.5 htpasswd

Name

htpasswd

Edit password files for user authentication

Synopsis

```
htpasswd [-c] passwdfile username
```

Description

This command enables you to edit the password file that is used for user authentication.

This command is used to specify the AuthUserFile directive parameter in the environment definition file (httpd.conf).

The options and parameters of this command are as follows:

-c

Creates a new user password file. If there is another file with the same name, it is overwritten. If this option is omitted, the user name is added to the file specified with *passwdfile*.

passwdfile

Specify a password file name.

username

Specify a maximum of 216 bytes for the user name. Alphanumeric characters, and symbols except those shown below, can be used.

- Colons (:)
- hash symbols (#)
- white spaces ()

Notes

- To delete a user, edit the password file by using a text editor.

The contents of the password file appear as follows when it is referenced using a text editor. To delete 'user2', delete the line containing 'user2' and save the file.

```
user1:$apr1$SR3.....$4aQAE2EU9NZTtbkxMEOa4/  
user2:$apr1$DS3.....$tEb4EYLhraAc1p2wIygTV/
```

- It is recommended that you change the access privileges for files created by this command:

Windows32/64

1. Start Windows Explorer.
2. Right-click the password file, and then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.
4. Select "Deny" for [Full control] for all groups except SYSTEM and Administrators.

Solaris32/64 Linux32/64

1. Login as superuser.
2. Change the file access privileges to "640".

```
chmod 640 <file>
```

3. Change the file owner to "root".

```
chown root <file>
```

4. Change the file group to "nobody" (the value set for the environment definition file (httpd.conf) Group directive).

```
chgrp nobody <file>
```

- As well as the -c option, the options for this command in Apache HTTP Server Version 2.2 can also be used. For details about these options, refer to the "Apache HTTP Server Version 2.2 Documentation".

Examples

Windows32/64

To create a new password file "C:\Interstage\F3FMahs\conf\password.txt", and register the password of user "user1":

```
C:\Interstage\F3FMahs\bin\htpasswd.exe -c C:\Interstage\F3FMahs\conf\password.txt user1  
New password:***** (*1)
```



```
Re-type new password:***** (*1)
Adding password for user user1
```

To add the password of user 'user2' to the same password file as above:

```
C:\Interstage\F3FMahs\bin\htpasswd.exe C:\Interstage\F3FMahs\conf\password.txt user2
New password:***** (*1)
Re-type new password:***** (*1)
Adding password for user user2
```

*1) Specify a maximum of 127 bytes for the password. Alphanumerics and symbols can be used.

Solaris32/64 **Linux32/64**

To create a new password file "/opt/FJSVahs/conf/password.txt", and register the password of user "user1":

```
/opt/FJSVahs/bin/htpasswd -c /opt/FJSVahs/conf/password.txt user1
New password:***** (*2)
Re-type new password:***** (*2)
Adding password for user user1
```

To add the password of user "user2" to the same password file as above:

```
/opt/FJSVahs/bin/htpasswd /opt/FJSVahs/conf/password.txt user2
New password:***** (*2)
Re-type new password:***** (*2)
Adding password for user user2
```

*1 Specify a maximum of 255 bytes for the password. Alphanumerics and symbols can be used.

7.6 httpd

Name

httpd

Start and stop the web server, and register and remove the web server services

Synopsis

Windows32/64

1. Starting the web server

```
httpd -k start [-n servicename]
```

2. Stopping the web server

```
httpd -k stop [-n servicename]
```

3. Registering the web server service

```
httpd -k install [-n servicename] [-f configfilename]
```

4. Removing the web server service

```
httpd -k uninstall [-n servicename]
```

Solaris32/64 **Linux32/64**

1. Starting the web server

```
httpd -k start [-f configfilename]
```

2. Stopping the web server

```
httpd -k stop [-f configfilename]
```

Description

This command starts and stops the web server, and registers and removes services.

The options and parameters of this command are as follows:

-k start | stop | install | uninstall

Specify the following parameters:

start

Specify when starting the web server.

stop

Specify when stopping the web server.

install Windows32/64

Specify when registering web server services.

uninstall Windows32/64

Specify when removing web server services.

-n servicename Windows32/64

Specify a maximum of 182 bytes for the service name. Alphanumeric characters, and symbols except those shown below, can be used.

- Slash (/)
- Backslash (\)

If this option is omitted, the default value will be "Apache2.2".

-f configfilename

Specifies the environment definition file (httpd.conf) with a full path.

If this option is omitted, the default value will be the following:

Windows32/64 (Default installation path)

```
C:\Interstage\F3FMahs\conf\httpd.conf
```

Solaris32/64 Linux32/64

```
/opt/FJSVahs/conf/httpd.conf
```

Notes

- Execute this command with administrator authority.

- Apart from the options above, the options for this command in Apache HTTP Server Version 2.2 can also be used. For details about these options, refer to the "Apache HTTP Server Version 2.2 Documentation".

However, the "restart" parameter and the "graceful" parameter of the -k option cannot be used when using the following features:

- Web Server Connector (for Interstage HTTP Server 2.2)
- Interstage Single Sign-on (Business server)
- **Windows32/64**
If you are registering a service by specifying "install" in the -k option, if Usage of this command is output after the message indicating successful registration of the service, it is possible that the option has been specified incorrectly. Specify the correct option and re-execute the command.

Example

Windows32/64

Starts the web server.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k start -n "Interstage HTTP Server 2.2"
```

Stops the web server.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k stop -n "Interstage HTTP Server 2.2"
```

Registers the web servers when creating multiple web servers.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k install -n "Service name"  
-f "<directory containing the web server resources>\conf\httpd.conf"
```

Removes the web server services when deleting multiple web servers.

```
C:\Interstage\F3FMahs\bin\httpd.exe -k uninstall -n "Service name"
```

Solaris32/64 Linux32/64

Starts the web server.

```
/opt/FJSVahs/bin/httpd -k start -f /opt/FJSVahs/conf/httpd.conf
```

Stops the web server.

```
/opt/FJSVahs/bin/httpd -k stop -f /opt/FJSVahs/conf/httpd.conf
```

7.7 **ihstregistupin**

Name

ihstregistupin

Register user PINs

Synopsis

```
ihsgregistupin -f upinfile -d slotdir
```

Description

The *ihsgregistupin* command registers a user PIN in the user PIN control file.

The created user PIN management file is defined in the SSLUserPINFile directive in the environment definition file (httpd.conf) of Interstage HTTP Server 2.2.

The options and parameters of this command are as follows:

-f upinfile

Specifies the user PIN control file that the encrypted user PIN is to be stored in.

-d slotdir

Specifies the slot information directory of the private-key control environment with an absolute path or a relative path.

User PIN Registration Procedure

1. Execute the user PIN registration command (*ihsgregistupin*).
2. When you are prompted for your user PIN, enter your user PIN with up to 128 characters (hidden).
3. When you are prompted for your user PIN again, enter the same user PIN as entered above (hidden).

Note

- Execute this command with administrator authority.
- Specify the character string of user PIN identical to the one that is used when the private-key control environment is created.
- The user PIN control file is overwritten and saved.
- It is recommended that this command is executed from consoles or from terminals connected by LANs which will not be accessed from outside, in order to prevent the user PIN from running on networks to leak out.
- **Windows32/64**
It is recommended that you change the access privileges for the user PIN file:

1. Start Windows Explorer.
2. Right-click the user PIN file, and then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.
4. Select "Deny" for [Full control] for all groups except SYSTEM and Administrators.

Example

Windows32/64

In this example, the user PIN is entered interactively, encrypted and registered in the "d:\ssl\upinfile" user PIN management file.

```
C:\Interstage\F3FMahs\bin\ihsgregistupin.exe -f d:\ssl\upinfile -d d:\sslenv\slot
UserPIN:
Re-type UserPIN:
```

Solaris32/64 Linux32/64

In this example, the user PIN is entered interactively, encrypted and registered in the "/home/ssl/upinfile" user PIN management file.

```
/opt/FJSVahs/bin/ihregistupin -f /home/ssl/upinfile -d /home/sslenv/slot
UserPIN:
Re-type UserPIN:
```

Chapter 8 Messages

This chapter provides the messages output by Interstage HTTP Server 2.2.

8.1 Messages Overview

8.1.1 Output Format

The output format of the messages is shown below:

Windows32/64

```
Label: Error type: Message number: Message text
```

Solaris32/64 Linux32/64

```
UX: Label: Error type: Message number: Message text
```



Note

UX appears at the beginning of all messages, but in this manual the UX has been omitted.

Label

Displays the service that output the message. Labels that can be displayed are shown below.

Label	Outline
AHS	Label output by Interstage HTTP Server 2.2

Error Type

Displays the status of the error in the message. The following error types are displayed:

Error Type	Outline
INFO	Displays the end status of the processing. No specific countermeasures are required.
WARNING	Shows an internal error. Refer to the User Action described in the message.
ERROR	Shows a fatal error. Refer to the User Action described in the message.

Message Number

Each message has its own unique ID number output to the screen or to an external device. Refer to this number to find its explanation in this manual.

Message Text

The message text describes the system status or error.

8.1.2 Before Contacting a Systems Engineer

Collecting data using the Batch Information Collection Tool

If a problem occurs while Interstage is running and it cannot be solved by following the procedure listed in "User Action", collect the necessary data using the *iscollectinfo* command, and then contact your systems engineer.

The *iscollectinfo* command is stored in the folder below:

Windows32/64 (Default installation path)

```
C:\Interstage\bin
```

Solaris32/64 (Default installation path) **Linux32/64**

```
/opt/FJSVisas/bin
```



.....
For details on the *iscollectinfo* command, refer to the "Maintenance Commands" chapter of the Reference Manual (Command Edition).
.....



.....
Using FJQSS (Information Collection Tool), the same information can be collected as using the *iscollectinfo* command.

For details on FJQSS, refer to the manual that is displayed from the following menu item:

- [Start] > [All Programs] > [FJQSS (Information Collection Tool)] > [FJQSS User's Guide]
-

8.2 ahs00000 to ahs00099

This section details the messages numbered between ahs00000 and ahs00099.

8.2.1 ahs00001

AHS: INFO: ahs00001: HTTP Server started. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server has been started.

8.2.2 ahs00002

AHS: INFO: ahs00002: HTTP Server stopped. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server has been stopped.

8.2.3 ahs00004

AHS: ERROR: ahs00004: Pre-configuration failed [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

An error occurred during initialization preprocessing.

System Action

The web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

8.2.4 ahs00005

AHS: ERROR: ahs00005: Unable to open logs [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

An error occurred during log initialization processing.

The File Descriptor number required to run the web server may be invalid.

System Action

The web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

8.2.5 ahs00006

AHS: ERROR: ahs00006: Configuration Failed [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

An error occurred during initialization processing.

System Action

The web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

8.2.6 ahs00008

AHS: ERROR: ahs00008: %s1: Module "%s2" is not compatible with this version of Apache (found %s3, need %s4). Please contact the vendor for the correct version. [%s5]

Variable Information

- %s1 = Web server program name
- %s2 = Plug-in module name
- %s3 = Plug-in module major version
- %s4 = Web server program major version
- %s5 = Environment definition file name

Explanation

The major version (%s4) of the web server program and the major version (%s3) of the plug-in module (%s2) are different.

System Action

The web server execution processing is aborted.

User Action

Check the major version of the plug-in module (%s2) specified in the LoadModule directive in the environment definition file (%s5).

8.2.7 ahs00009

AHS: ERROR: ahs00009: %s1: Module "%s2" could not be loaded, because the dynamic module limit was reached. Please increase DYNAMIC_MODULE_LIMIT and recompile. [%s3]

Variable Information

- %s1 = Web server program name
- %s2 = Plug-in module name
- %s3 = Environment definition file name

Explanation

The maximum number of plug-in modules that can be used has been exceeded.

System Action

The web server execution processing is aborted.

User Action

Check whether 129 or more LoadModule directives have been set in the environment definition file (%s3). A maximum of 128 LoadModule directives can be set.

8.2.8 ahs00010

AHS: ERROR: ahs00010: Syntax error in -C/-c directive: %s1 [%s2]

Variable Information

- %s1 = Syntax error description
- %s2 = Environment definition file name

Explanation

The syntax of the directive specified for the -C or -c option is incorrect.

System Action

The web server execution processing is aborted.

User Action

Check the syntax of the directive specified for the -C or -c options.

8.2.9 ahs00011

AHS: ERROR: ahs00011: %s1: Could not open configuration file %s2: %s3 [%s2]

Variable Information

%s1 = Web server program name

%s2 = Environment definition file name

%s3 = Error details information

Explanation

The environment definition file (%s2) could not be opened.

System Action

The web server execution processing is aborted.

User Action

Check whether the environment definition file (%s2) exists.

8.2.10 ahs00012

AHS: ERROR: ahs00012: %s1 Syntax error on line %s2 of %s3: %s4 [%s3]

Variable Information

%s1 = Web server program name

%s2 = The line in the environment definition file

%s3 = Environment definition file name

%s4 = Syntax error description



Note

.....
The web server program name (%s1) may not be output.
.....

Explanation

Syntax error (%s4) occurred in the environment definition file (%s3).

System Action

The web server execution processing is aborted.

User Action

Reexamine the environment definition file (%s3) by referring to the explanation of syntax error (%s4).

8.2.11 ahs00013

AHS: ERROR: ahs00013: (%s1)%s2: Invalid config file path %s3 [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The specified environment definition file (%s3) path is incorrect.

System Action

The web server execution processing is aborted.

User Action

Check the path of the specified environment definition file (%s3).

8.2.12 ahs00014

AHS: ERROR: ahs00014: (%s1)%s2: alloc_listener: failed to set up sockaddr for %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

%s4 = Environment definition file name

Explanation

The host (%s3) information specified for the Listen directive in the environment definition file (%s4) could not be found.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.13 ahs00015

AHS: ERROR: ahs00015: (%s1)%s2: alloc_listener: failed to get a socket for %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

%s4 = Environment definition file name

Explanation

A communication socket could not be created.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.14 ahs00016

AHS: ERROR: ahs00016: (%s1)%s2: make_sock: for address %s3, apr_socket_opt_set: (%s4) [%s5]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = IP address:Port number
- %s4 = Socket option
- %s5 = Environment definition file name

Explanation

The socket option (%s4) could not be set.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.15 ahs00017

AHS: WARNING: ahs00017: (%s1)%s2: make_sock: failed to set %s3 for address %s4, using default [%s5]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = IP address:Port number
- %s4 = Socket option
- %s5 = Environment definition file name

Explanation

The socket option (%s4) could not be set. The socket option runs using the system default value.

System Action

The web server start processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.16 ahs00018

AHS: ERROR: ahs00018: (%s1)%s2: make_sock: could not bind to address %s3 [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = IP address:Port number
- %s4 = Environment definition file name

Explanation

An address could not be assigned to the socket.

System Action

The web server start processing is canceled.

User Action

Take the action described in table below, according to Error details number (%s1).

Error details number (%s1)	Meaning/Required Action	Remark
<div style="border: 1px solid black; padding: 2px;">Windows32/64</div> OS 10013 OS 10048	If this message is output when the web server starts, take one of the following actions: <ul style="list-style-type: none"> - If the web server was restarted immediately after being stopped, the release processing for the IP address or the port number (%s3) used by the web server that was stopped may not have completed. Wait for a while (several seconds), and then restart the web server. - Another service is using the IP address and port number (%s3) or port number (%s3). Check whether the IP address and port number specified for the web server is also specified for another service. If so, terminate that service, or use a different IP address and/or port number. If the IP address and port number settings are correct, collect diagnostic information with the <i>iscollectinfo</i> command, and contact your SE (systems engineer). - If more than one Listen directive with the same IP address and port number combination has been set in the environment definition file (%s4), delete the one that is not needed. 	<div style="border: 1px solid black; padding: 2px;">Windows32/64</div> <div style="border: 1px solid black; padding: 2px;">Linux32/64</div> (*1)
<div style="border: 1px solid black; padding: 2px;">Solaris32/64</div> 125		
<div style="border: 1px solid black; padding: 2px;">Linux32/64</div> 98		
<div style="border: 1px solid black; padding: 2px;">Windows32/64</div> OS 10049	An invalid address was specified. Check the settings of the Listen directive in the environment definition file (%s4).	
<div style="border: 1px solid black; padding: 2px;">Solaris32/64</div> 126		
<div style="border: 1px solid black; padding: 2px;">Linux32/64</div> 22 99		
<div style="border: 1px solid black; padding: 2px;">Linux32/64</div> 99	The IP address (%3) was mapped to an invalid network interface. Check the settings of the network interface to which the IP address (%3) was mapped. If the settings are correct, collect diagnostic information with the <i>iscollectinfo</i> command, and contact your SE (systems engineer) .	
All other cases	Resolve the cause of the error according to the error details context (%s2).	

*1: If an IP address has not been specified in the Listen directive of the environment definition file (%s4), the following messages may be output in succession:

- A message with the IP address:Port number (%s3) where the IP address is "[::]"
- A message with the IP address:Port number (%s3) where the IP address is "0.0.0.0"

8.2.17 ahs00019

AHS: ERROR: ahs00019: (%s1)%s2: make_sock: unable to listen for connections on address %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

%s4 = Environment definition file name

Explanation

Socket wait status transition failed.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.18 ahs00020

AHS: ERROR: ahs00020: no listening sockets available, shutting down [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

A valid Listen directive has not been set in the environment definition file (%s1).

System Action

The web server execution processing is aborted.

User Action

If the Listen directive has not been set in the environment definition file (%s1), set it. If the Listen directive has been set, refer to the message that was output at the same time and fix the error.

8.2.19 ahs00021

AHS: ERROR: ahs00021: (%s1)%s2: Couldn't start ErrorLog process [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The log output program specified for the ErrorLog directive in the environment definition file (%s3) could not be started.

System Action

The web server execution processing is aborted.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the ErrorLog directive that is set in the environment definition file (%s3).

8.2.20 ahs00022

AHS: ERROR: ahs00022: (%s1)%s2: %s3: Invalid error log path %s4. [%s5]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Web server program name
- %s4 = Error log file name
- %s5 = Environment definition file name

Explanation

The path of the error log file (%s4) could not be found.

System Action

The web server execution processing is aborted.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the path of the error log file (%s4) specified for the ErrorLog directive in the environment definition file (%s5).

8.2.21 ahs00023

AHS: ERROR: ahs00023: (%s1)%s2: %s3: could not open error log file %s4. [%s5]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Web server program name
- %s4 = Error log file name
- %s5 = Environment definition file name

Explanation

The error log file (%s4) specified for the ErrorLog directive in the environment definition file (%s5) could not be opened.

System Action

The web server execution processing is aborted.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check that the error log file (%s4) specified for the ErrorLog directive in the environment definition file (%s5) is correct.

8.2.22 ahs00024

AHS: ERROR: ahs00024: piped_log_spawn: unable to setup child process '%s1': %s2 [%s3]

Variable Information

- %s1 = Log output program name
- %s2 = Error details context
- %s3 = Environment definition file name

Explanation

Initialization processing for the log output program (%s1) failed.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.23 ahs00025

AHS: ERROR: ahs00025: unable to start piped log program '%s1': %s2 [%s3]

Variable Information

%s1 = Log output program name

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The log output program (%s1) could not be started.

System Action

The web server execution processing is aborted.

User Action

Take the action described in table below, according to the error details context (%s2).

Error details context (%s2)	Meaning/Required Action
Windows32/64 The paging file is too small for this operation to complete	The desktop heap may be depleted. If the desktop heap is depleted, extend the desktop heap.
Windows32/64 Attempt to access invalid address	
Windows32/64 Unrecognized Win32 error code 14001	
Windows32/64 Insufficient system resources exist to complete the requested service.	
All other cases	Resolve the cause of the error according to the error details context (%s2).

8.2.24 ahs00026

AHS: ERROR: ahs00026: (%s1)%s2: Invalid PID file path %s3, ignoring. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process management file name

%s4 = Environment definition file name

Explanation

The path of the process management file (%s3) could not be found.

System Action

The web server start processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check that the process management file (%s3) specified for the PidFile directive in the environment definition file (%s4) is correct.

8.2.25 ahs00028

AHS: ERROR: ahs00028: %s1: could not log pid to file %s2 [%s3]

Variable Information

%s1 = Web server program name

%s2 = Process management file name

%s3 = Environment definition file name

Explanation

The process management file (%s1) could not be opened.

System Action

The web server start processing is continued.

User Action

Check that the process management file (%s2) specified for the PidFile directive in the environment definition file (%s3) is correct.

8.2.26 ahs00029

AHS: ERROR: ahs00029: [%s1] file %s2, line %s3, assertion "%s4" failed [%s5]

Variable Information

%s1 = Time of occurrence

%s2 = Source file name

%s3 = Source file line number

%s4 = Details information

%s5 = Environment definition file name

Explanation

An error occurred in the web server.

System Action

The web server execution processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.2.27 ahs00030

AHS: ERROR: ahs00030: (%s1)%s2: Fatal error: unable to create global pool for use with by the scoreboard [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The memory management area that is used in scoreboard management could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.28 ahs00031

AHS: ERROR: ahs00031: (%s1)%s2: Fatal error: Invalid Scoreboard path %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Scoreboard file path

%s4 = Environment definition file name

Explanation

The path of the scoreboard file (%s3) could not be found.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.29 ahs00032

AHS: ERROR: ahs00032: (%s1)%s2: Unable to create or access scoreboard (anonymous shared memory failure) [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The shared memory that is used in the scoreboard could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.30 ahs00033

AHS: ERROR: ahs00033: (%s1)%s2: cannot allocate scoreboard [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The memory that is used in the scoreboard could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.31 ahs00034

AHS: ERROR: ahs00034: (%s1)%s2: unable to create or access scoreboard "%s3" (name-based shared memory failure) [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Scoreboard name

%s4 = Environment definition file name

Explanation

The shared memory that is used in the scoreboard (%s3) could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.32 ahs00035

AHS: ERROR: ahs00035: (%s1)%s2: invalid transfer log path %s3. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Access log file name

%s4 = Environment definition file name

Explanation

The path of the access log file (%s3) could not be found.

System Action

The web server program execution processing is aborted.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the CustomLog directive and the TransferLog directive that is set in the environment definition file (%s4).

8.2.33 ahs00036

AHS: ERROR: ahs00036: (%s1)%s2: could not open transfer log file %s3. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Access log file name

%s4 = Environment definition file name

Explanation

The access log file (%s3) could not be opened.

System Action

The web server execution processing is aborted.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the CustomLog directive and the TransferLog directive that is set in the environment definition file (%s4).

8.2.34 ahs00037

AHS: ERROR: ahs00037: (%s1)%s2: Invalid mime types config path %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = MIME type settings file name

%s4 = Environment definition file name

Explanation

The path of the MIME type settings file (%s3) could not be found.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the TypesConfig directive that is set in the environment definition file (%s4).

8.2.35 ahs00038

AHS: ERROR: ahs00038: (%s1)%s2: could not open mime types config file %s3. [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = MIME type settings file name
- %s4 = Environment definition file name

Explanation

The MIME type settings file (%s3) could not be opened.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the TypesConfig directive that is set in the environment definition file (%s4).

8.2.36 ahs00040

AHS: ERROR: ahs00040: (%s1)%s2: mod_rewrite: Parent could not create RewriteLock file %s3 [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Name of the lock file for the rewrite function
- %s4 = Environment definition file name

Explanation

The lock file (%s3) for the rewrite function could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.37 ahs00041

AHS: ERROR: ahs00041: (%s1)%s2: mod_unique_id: unable to find hostname of the server [%s3]

Variable Information

- %s1 = Error details number
- %s2 = Error details context

%s3 = Environment definition file name

Explanation

The host name could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.38 ahs00042

AHS: ERROR: ahs00042: (%s1)%s2: mod_unique_id: unable to find IPv4 address of "%s3" [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

%s4 = Environment definition file name

Explanation

The name of Host (%s3) could not be resolved.

System Action

Windows32/64

The web server execution processing is continued.

Solaris32/64 Linux32/64

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.2.39 ahs00043

AHS: WARNING: ahs00043: Require %s1 > 0, setting to 1 [%s2]

Variable Information

%s1 = Directive name

%s2 = Environment definition file name

Explanation

A value of "0" or less was set for the directive (%s1) in the environment definition file (%s2). The directive (%s1) requires a value of "1".

System Action

The web server execution processing is continued.

User Action

Set a value of "1" or more for the directive (%s1) in the environment definition file (%s2).

8.2.40 ahs00044

Windows32/64

AHS: WARNING: ahs00044: ThreadLimit of %s1 exceeds compile time limit of %s2 threads, lowering ThreadLimit to %s2. [%s3]

Solaris32/64 Linux32/64

AHS: WARNING: ahs00044: ThreadLimit of %s1 exceeds compile time limit of %s2 servers, lowering ThreadLimit to %s2. [%s3]

Variable Information

%s1 = The value set for the ThreadLimit directive

%s2 = Limit for the ThreadLimit directive

%s3 = Environment definition file name

Explanation

The value (%s1) set for the ThreadLimit directive in the environment definition file (%s3) has exceeded the limit (%s2). The ThreadLimit directive requires a value of limit (%s2) to be set.

System Action

The web server execution processing is continued.

User Action

Set a value that does not exceed the limit (%s2) for the ThreadLimit directive in the environment definition file (%s3).

8.2.41 ahs00045

AHS: WARNING: ahs00045: ThreadsPerChild of %s1 exceeds ThreadLimit value of %s2 threads, lowering ThreadsPerChild to %s2. To increase, please see the ThreadLimit directive. [%s3]

Variable Information

%s1 = The value set for the ThreadsPerChild directive

%s2 = Limit for the ThreadsPerChild directive

%s3 = Environment definition file name

Explanation

The value (%s1) set for the ThreadsPerChild directive in the environment definition file (%s3) has exceeded the limit (%s2). The ThreadsPerChild directive requires a value of limit (%s2) to be set.

System Action

The web server execution processing is continued.

User Action

Set a value that does not exceed the limit (%s2) for the ThreadsPerChild directive in the environment definition file (%s3).

8.3 ahs00100 to ahs00199

This section details the messages numbered between ahs00100 and ahs00199.

8.3.1 ahs00100

AHS: ERROR: ahs00100: (%s1)%s2: Failed to get the full path of %s3 [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Web server program name
- %s4 = Environment definition file name

Explanation

The full path of the web server program (%s3) could not be found.

System Action

The web server program execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.2 ahs00101

AHS: ERROR: ahs00101: %s1: Service is already installed. [%s2]

Variable Information

- %s1 = Service name
- %s2 = Environment definition file name

Explanation

The web server service (%s1) has already been registered.

System Action

The web server service registration processing is aborted.

User Action

Check the service (%s1) registration status in the Services window ([Control Panel] > [Administrative Tools] > [Services]).

8.3.3 ahs00102

AHS: ERROR: ahs00102: (%s1)%s2: No installed service named "%s3".

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Service name



.....
The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.
.....

Explanation

The web server service (%s3) has not been registered.

System Action

The web server program execution processing is aborted.

User Action

Check if the service name (%s3) specified in the [httpd](#) command is correct.

If the service name (%s3) is incorrect, specify the correct service name in the [httpd](#) command, and then reexecute the command.

If the service name (%s3) is correct, collect diagnostic information using the [iscollectinfo](#) command, and then [contact your SE \(systems engineer\)](#).

8.3.4 ahs00103

AHS: ERROR: ahs00103: (%s1)%s2: %s3: Unable to start the service manager. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

%s4 = Environment definition file name

Explanation

The service control manager could not be started.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.5 ahs00104

AHS: ERROR: ahs00104: (%s1)%s2: Parent: Cannot create shutdown event %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

%s4 = Environment definition file name

Explanation

The shutdown event object (%s3) could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.6 ahs00105

AHS: ERROR: ahs00105: (%s1)%s2: Parent: Cannot create restart event %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

%s4 = Environment definition file name

Explanation

The restart event object (%s3) could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.7 ahs00106

AHS: ERROR: ahs00106: (%s1)%s2: %s3: Unable to create the start_mutex. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

%s4 = Environment definition file name

Explanation

Exclusive resources for the daemon process could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.8 ahs00107

AHS: ERROR: ahs00107: (%s1)%s2: master_main: create child process failed. Exiting. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name



.....
The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.
.....

Explanation

An error occurred in daemon process create processing.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

8.3.9 ahs00108

AHS: ERROR: ahs00108: (%s1)%s2: master_main: WaitForMultipleObjects WAIT_FAILED -- doing server shutdown [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

An error occurred in daemon process status monitoring.

System Action

The web server program execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.10 ahs00109

AHS: ERROR: ahs00109: (%s1)%s2: master_main: WaitForMultipleObjects with INFINITE wait exited with WAIT_TIMEOUT [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A timeout occurred in daemon process status monitoring.

System Action

The web server program execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.11 ahs00111

AHS: ERROR: ahs00111: Parent: child process exited with status %s1 -- Aborting. [%s2]

Variable Information

%s1 = Daemon process exit code

%s2 = Environment definition file name

Explanation

An error occurred in the daemon process.

System Action

The web server program execution processing is aborted.

User Action

Refer to the message or error logs output at the same time and fix the error.

8.3.12 ahs00112

AHS: ERROR: ahs00112: (%s1)%s2: GetModuleFileName failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The full path of the web server program could not be acquired.

System Action

The web server service registration processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.13 ahs00113

AHS: ERROR: ahs00113: (%s1)%s2: Failed to open the WinNT service manager. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name



.....
The environment definition file name (%s3) "[%s3]" may not be output.
.....

Explanation

A connection could not be established with the service control manager.

System Action

The web server program execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.14 ahs00114

AHS: ERROR: ahs00114: (%s1)%s2: OpenService failed [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name



The environment definition file name (%s3) "[%s3]" may not be output.

Explanation

The web server service could not be opened.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.15 ahs00115

AHS: ERROR: ahs00115: (%s1)%s2: ChangeServiceConfig failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The web server service configuration parameter could not be modified.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.16 ahs00116

AHS: ERROR: ahs00116: (%s1)%s2: Failed to create WinNT Service Profile

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The web server service could not be registered.

System Action

The web server service registration processing is aborted.

User Action

Check if the service name specified during the registration processing of the web server service contains a string with a slash (/) or backslash (\).

If a slash (/) or backslash (\) is specified in the service name, specify the correct service name for the [httpd](#) command and execute the command again.

If a slash (/) or backslash (\) is not specified in the service name, resolve the cause of the error according to the error details context (%s2).

8.3.17 ahs00117

AHS: ERROR: ahs00117: (%s1)%s2: %s3: Failed to store the ConfigArgs in the registry.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The registry for the option used when the web server service (%s3) starts could not be registered.

System Action

The web server service registration processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.18 ahs00118

AHS: ERROR: ahs00118 (%s1)%s2: %s3: Failed to delete the service.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service (%s3) could not be deleted.

System Action

The web server service deletion processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.19 ahs00119

AHS: ERROR: ahs00119: (%s1)%s2: Query of Service %s3 failed

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service (%s3) status could not be obtained.

System Action

The web server stop processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.20 ahs00120

AHS: ERROR: ahs00120: (%s1)%s2: ISAPI: could not create the isapi cache pool [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The memory management area for the mod_isap module could not be created.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.21 ahs00123

AHS: ERROR: ahs00123: (%s1)%s2: Parent: Failed to get full path of %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Web server program name

%s4 = Environment definition file name

Explanation

The path of the web server program (%s3) could not be found.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.22 ahs00124

AHS: ERROR: ahs00124: (%s1)%s2: Parent: Unable to %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Erroneous processing contents

%s4 = Environment definition file name

Explanation

Failed to copy the start event handle.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.23 ahs00125

AHS: ERROR: ahs00125: (%s1)%s2: Parent: Could not create %s3 event for child process [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event type

%s4 = Environment definition file name

Explanation

An event object could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.24 ahs00126

AHS: ERROR: ahs00126: (%s1)%s2: Parent: Failed to create the child process. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A daemon process could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.25 ahs00127

AHS: ERROR: ahs00127: (%s1)%s2: Parent: WSADuplicateSocket failed for socket %s3. Check the FAQ. [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Socket descriptor
- %s4 = Environment definition file name

Explanation

The socket could not be reproduced.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.26 ahs00128

AHS: ERROR: ahs00128: (%s1)%s2: %s3: Failed to start the service process. [%s4]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Service name
- %s4 = Environment definition file name

Explanation

The web server service (%s3) could not be started.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

8.3.27 ahs00129

AHS: ERROR: ahs00129: (%s1)%s2: Child %s3: _beginthreadex failed. Unable to create all worker threads. Created %s4 of the %s5 threads requested with the ThreadsPerChild configuration directive. [%s6]

Variable Information

- %s1 = Error details number
- %s2 = Error details context
- %s3 = Process ID of the daemon process
- %s4 = The number of created communication threads
- %s5 = The value set for the ThreadsPerChild directive
- %s6 = Environment definition file name

Explanation

The communication thread could not be created.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.28 ahs00130

AHS: INFO: ahs00130: Parent: child process exited with status %s1 -- Restarting. [%s2]

Variable Information

%s1 = Process ID of the daemon process

%s2 = Environment definition file name

Explanation

The daemon process is restarted.

8.3.29 ahs00131

AHS: WARNING: ahs00131: Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The number of simultaneous connection requests from the client has exceeded the value set for the ThreadsPerChild directive in the environment definition file (%s1) (maximum number of requests).



.....
This message is output the first time the number of requests exceeds the maximum value for the number of simultaneous connections after the web server starts up. Once this message is output, it is not output again until the web server restarts.
.....

System Action

The web server execution processing is continued.

User Action

If necessary, check the value set for the ThreadsPerChild directive in the environment definition file (%s1) (maximum number of requests).

8.3.30 ahs00132

AHS: ERROR: ahs00132: (%s1)%s2: OpenEvent on %s3 event [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

%s4 = Environment definition file name

Explanation

The event object (%s3) could not be opened.

System Action

The web server execution processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.3.31 ahs00133

AHS: ERROR: ahs00133: (%s1)%s2: SetEvent on %s3 event [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

%s4 = Environment definition file name

Explanation

Failed to set the signal status of the event object (%s3).

System Action

The web server execution processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.3.32 ahs00134

AHS: ERROR: ahs00134: (%s1)%s2: Parent: Failed to get the current path [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to retrieve the current path.

System Action

The web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.33 ahs00135

AHS: ERROR: ahs00135: (%s1)%s2: Parent: Could not set child process stdout [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to change the configuration for the standard output of the daemon process.

System Action

The web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.34 ahs00136

AHS: ERROR: ahs00136: (%s1)%s2: Parent: Could not set child process stderr [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to change the configuration for the standard error output of the daemon process.

System Action

The web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.35 ahs00137

AHS: ERROR: ahs00137: (%s1)%s2: ResetEvent(shutdown_event) [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to reset the event object used for shutdown.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.36 ahs00138

AHS: ERROR: ahs00138: (%s1)%s2: Parent: ResetEvent(restart_event) failed. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to reset the event object used for restart.

System Action

The web server is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.37 ahs00139

AHS: ERROR: ahs00139: (%s1)%s2: Parent: SetEvent for child process %s3 failed [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Daemon process handle

%s4 = Environment definition file name

Explanation

Failed to set the signal status of the event object used for stopping the daemon process.

System Action

The web server is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.38 ahs00140

AHS: WARNING: ahs00140: (%s1)%s2: No installed ConfigArgs for the service "%s3", using Apache defaults.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

Failed to retrieve the contents of the ConfigArgs registry for the service (%s3).

System Action

The web server execution processing is continued.

8.3.39 ahs00141

AHS: ERROR: ahs00141: (%s1)%s2: Failure registering service handler**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to register the function that processes the service control request.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.3.40 ahs00142

AHS: ERROR: ahs00142: (%s1)%s2: Error starting service control dispatcher**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to set the service control dispatcher thread.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4 ahs00200 to ahs00299

This section details the messages numbered between ahs00200 and ahs00299.

8.4.1 ahs00200

AHS: ERROR: ahs00200: (%s1)%s2: Error retrieving pid file %s3 [%s4]**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Process management file

%s4 = Environment definition file name

Explanation

The process management file (%s3) could not be read.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.2 ahs00201

AHS: WARNING: ahs00201: httpd (pid %s1) already running [%s2]

Variable Information

%s1 = Process ID

%s2 = Environment definition file name

Explanation

The web server is already running.

System Action

The web server start processing is canceled.

8.4.3 ahs00202

AHS: WARNING: ahs00202: httpd (no pid file) not running [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server is not running.

System Action

The web server stop processing is canceled.

8.4.4 ahs00203

AHS: WARNING: ahs00203: httpd (pid %s1?) not running [%s2]

Variable Information

%s1 = Process ID

%s2 = Environment definition file name

Explanation

The web server process (%s1) does not exist.

System Action

The web server stop processing is canceled.

8.4.5 ahs00204

AHS: WARNING: ahs00204: httpd not running, trying to start [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server is not running.

System Action

The web server start processing is started.

8.4.6 ahs00205

AHS: ERROR: ahs00205: (%s1)%s2: sending signal to server [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The signal failed to be sent to the daemon process.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.7 ahs00206

AHS: ERROR: ahs00206: Child %s1 returned a Fatal error... Apache is exiting! [%s2]

Variable Information

%s1 = Process ID of the communication process

%s2 = Environment definition file name

Explanation

An error occurred in the communication process (%s1).

System Action

The web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

8.4.8 ahs00207

AHS: ERROR: ahs00207: (%s1)%s2: apr_proc_detach failed [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A daemon process could not be generated.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.9 ahs00208

AHS: ERROR: ahs00208: (%s1)%s2: Could not open pipe-of-death. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A pipe could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.10 ahs00209

AHS: ERROR: ahs00209: (%s1)%s2: Couldn't create accept lock [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Exclusive resources for connection could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.11 ahs00210

AHS: ERROR: ahs00210: (%s1)%s2: Couldn't set permissions on cross-process lock; check User and Group directives [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Authority failed to be set for exclusive resources for connection.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.12 ahs00213

AHS: ERROR: ahs00213: (%s1)%s2: Couldn't initialize cross-process lock in child [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Exclusive resources for connection could not be initialized.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.13 ahs00214

AHS: ERROR: ahs00214: (%s1)%s2: setuid: unable to change to uid: %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID

%s4 = Environment definition file name

Explanation

The User ID (%s3) specified for the User directive in the environment definition file (%s4) could not be set.

System Action

The communication process where the error occurred is closed, and the web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check User ID (%s3) specified by the User directive in the environment definition file (%s4).

8.4.14 ahs00215

AHS: ERROR: ahs00215: (%s1)%s2: getpwuid: couldn't determine user name from uid %s3, you probably need to modify the User directive [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID

%s4 = Environment definition file name



Error details number (%s1) and Error details context (%s2) "(%s1)%s2:" may not be output.

Explanation

The User ID (%s3) entry specified for the User directive in the environment definition file (%s4) could not be found.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the User ID (%s3) specified by the User directive in the environment definition file (%s4).

8.4.15 ahs00216

AHS: ERROR: ahs00216: (%s1)%s2: setgid: unable to set group id to Group %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Group ID

%s4 = Environment definition file name

Explanation

The Group ID (%s3) specified for the Group directive in the environment definition file (%s4) could not be set.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the Group ID (%s3) specified by the Group directive in the environment definition file (%s4).

8.4.16 ahs00217

AHS: ERROR: ahs00217: (%s1)%s2: initgroups: unable to set groups for User %s3 and Group %s4 [%s5]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID

%s4 = Group ID

%s5 = Environment definition file name

Explanation

The group access list could not be initialized.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.17 ahs00219

AHS: ERROR: ahs00219: (%s1)%s2: mod_rewrite: Parent could not set permissions on RewriteLock; check User and Group directives [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The authority for the lock file for the rewrite function could not be set.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.18 ahs00221

AHS: WARNING: ahs00221: MaxClients of %s1 would require %s2 servers, and would exceed the ServerLimit value of %s3. Automatically lowering MaxClients to %s4. To increase, please see the ServerLimit directive. [%s5]

Variable Information

%s1 = The value set for the MaxClients directive

%s2 = The maximum number of communication processes

%s3 = The value set for the ServerLimit directive

%s4 = Limit for the MaxClients directive

%s5 = Environment definition file name

Explanation

The value (%s1) set for the MaxClients directive in the environment definition file (%s5) has exceeded the limit (%s4). The MaxClients directive requires a value of limit (%s4).

System Action

The web server execution processing is continued.

User Action

Set a value that does not exceed the limit (%s4) for the MaxClients directive in the environment definition file (%s5).

8.4.19 ahs00222

AHS: WARNING: ahs00222: ServerLimit of %s1 exceeds compile time limit of %s2 servers, lowering ServerLimit to %s2. [%s3]

Variable Information

%s1 = The value set for the ServerLimit directive

%s2 = Limit for the ServerLimit directive

%s3 = Environment definition file name

Explanation

The value (%s1) set for the ServerLimit directive in the environment definition file (%s3) has exceeded the limit (%s2). The ServerLimit directive requires a value of limit (%s2).

System Action

The web server execution processing is continued.

User Action

Set a value that does not exceed the limit (%s2) for the ServerLimit directive in the environment definition file (%s3).

8.4.20 ahs00223

AHS: ERROR: ahs00223: %s1: bad user name %s2 [%s3]

Variable Information

%s1 = Web server program name

%s2 = User name specified in the User directive

%s3 = Environment definition file name

Explanation

The user name (%s2) specified in the User directive of the environment definition file (%s3) could not be found.

System Action

The web server program execution processing is aborted.

User Action

Check whether the user name (%s2) specified in the User directive of the environment definition file (%s3) is registered.

8.4.21 ahs00224

AHS: ERROR: ahs00224: %s1: bad group name %s2 [%s3]

Variable Information

%s1 = Web server program name

%s2 = Group name specified in the Group directive

%s3 = Environment definition file name

Explanation

The group name (%s2) specified in the Group directive of the environment definition file (%s3) could not be found.

System Action

The web server execution processing is aborted.

User Action

Check whether the group name (%s2) specified in the Group directive of the environment definition file (%s3) is registered.

8.4.22 ahs00227

AHS: ERROR: ahs00227: (%s1)%s2: unable to control socket non-blocking status [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The non-blocking of the socket failed.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.23 ahs00228

AHS: WARNING: ahs00228: server reached MaxClients setting, consider raising the MaxClients setting [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The number of simultaneous connection requests from the client has exceeded the value (maximum number of requests) set for the MaxClients directive in the environment definition file (%s1).



Note

.....
This message is output the first time the number of requests exceeds the maximum value for the number of simultaneous connections after the web server starts up. Once this message is output, it is not output again until the web server restarts.
.....

System Action

The web server execution processing is continued.

User Action

If necessary, check the value (maximum number of requests) set for the MaxClients directive in the environment definition file (%s1).

8.4.24 ahs00229

AHS: ERROR: ahs00229: (%s1)%s2: apr_thread_create: unable to create listener thread [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

The thread could not be created.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.25 ahs00230

AHS: ERROR: ahs00230: (%s1)%s2: Couldn't initialize signal thread [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to initialize the thread signal.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.26 ahs00231

AHS: ERROR: ahs00231: (%s1)%s2: fork: Unable to fork new process [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A communication process could not be created.

System Action

The web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.27 ahs00232

AHS: ERROR: ahs00232: (%s1)%s2: Cannot chroot when not started as root [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Unable to retrieve the user ID that starts the daemon process.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.28 ahs00233

AHS: ERROR: ahs00233: (%s1)%s2: Can't chdir to %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Directory name

%s4 = Environment definition file name

Explanation

Unable to change the current directory to the directory (%s3).

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Check the ChrootDir directive that is set in the environment definition file (%s4).

8.4.29 ahs00234

AHS: ERROR: ahs00234: (%s1)%s2: Can't chroot to %s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Directory name

%s4 = Environment definition file name

Explanation

Unable to change the root directory to the directory (%s3).

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.30 ahs00235

AHS: ERROR: ahs00235: (%s1)%s2: apr_socket_accept: giving up. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

A network error was detected.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.31 ahs00236

AHS: ERROR: ahs00236: (%s1)%s2: apr_socket_accept: (client socket) [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

An attempt to connect to the client socket failed.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.32 ahs00237

AHS: ERROR: ahs00237: (%s1)%s2: ap_queue_init() failed [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to initialize the internal queue.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.33 ahs00238

AHS: ERROR: ahs00238: (%s1)%s2: ap_queue_info_create() failed [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to create the communication queue.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.34 ahs00239

AHS: ERROR: ahs00239: (%s1)%s2: malloc: out of memory [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Memory could not be obtained.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.35 ahs00240

AHS: ERROR: ahs00240: (%s1)%s2: apr_thread_create: unable to create worker thread [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name

Explanation

Failed to create the communication thread.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

8.4.36 ahs00241

AHS: WARNING: ahs00241: detected MinSpareThreads set to non-positive. Resetting to 1 to avoid almost certain Apache failure. Please read the documentation. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

A value of "0" or less was set for the MinSpareThreads directive in the environment definition file (%s1). The MinSpareThreads directive requires a value of "1".

System Action

The web server execution processing is continued.

User Action

Set a value of "1" or more for the MinSpareThreads directive in the environment definition file (%s1).

8.4.37 ahs00242

AHS: WARNING: ahs00242: MaxClients (%s1) must be at least as large as ThreadsPerChild (%s2). Automatically increasing MaxClients to %s2. [%s3]

Variable Information

%s1 = The value set for the MaxClients directive

%s2 = The value set for the ThreadsPerChild directive

%s3 = Environment definition file name

Explanation

A value set for the ThreadsPerChild directive or less was set for the MaxClients directive in the environment definition file (%s3). The MaxClients directive requires a value set for the ThreadsPerChild directive.

System Action

The web server execution processing is continued.

User Action

Set a value set for the ThreadsPerChild directive or more for the MaxClients directive in the environment definition file (%s3).

8.4.38 ahs00243

AHS: WARNING: ahs00243: MaxClients (%s1) is not an integer multiple of ThreadsPerChild (%s2), lowering MaxClients to %s3 for a maximum of %4 child processes, [%s5]

Variable Information

- %s1 = The value set for the MaxClients directive
- %s2 = The value set for the ThreadsPerChild directive
- %s3 = Limit for the MaxClients directive
- %s4 = The maximum number of communication processes
- %s5 = Environment definition file name

Explanation

The value set for the MaxClients directive (%s1) in the environment definition file (%s5) is not an integer multiple of the value set for the ThreadsPerChild directive (%s2). The MaxClients directive uses the limit value (%s3).

System Action

The web server execution processing is continued.

User Action

As the value to be set for the MaxClients directive in the environment definition file (%s5), set an integer multiple of the value set for the ThreadsPerChild directive.

8.4.39 ahs00244

AHS: ERROR: ahs00244: No active workers found... Apache is exiting! [%s1]

Variable Information

- %s1 = Environment definition file name

Explanation

There are no active communication threads.

System Action

The web server execution processing is aborted.

User Action

Collect troubleshooting information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.4.40 ahs00245

AHS: INFO: ahs00245: seg fault or similar nasty error detected in the parent process [%s1]

Variable Information

- %s1 = Environment definition file name

Explanation

- The daemon process received one of the following signals:
 - SIGSEGV
 - SIGBUS
 - SIGABORT
 - SIGABRT

- SIGILL

System Action

The daemon process is closed.

User Action

Collect troubleshooting information using the `iscollectinfo` command, and [contact your SE \(systems engineer\)](#).

8.5 ahs00400 to ahs00499

This section details the messages numbered between ahs00400 and ahs00499.

8.5.1 ahs00401

AHS: ERROR: ahs00401: (%s1)%s2: Couldn't start TraceLog process. [%s3]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file name



.....
The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.
.....

Explanation

The log output program specified for the TraceLog directive in the environment definition file (%s3) could not be started.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Refer to the message that was output at the same time and fix the error.
- Check the TraceLog directive that is set in the environment definition file (%s3).

8.5.2 ahs00402

AHS: ERROR: ahs00402: (%s1)%s2: Invalid TraceLog file path %s3. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Name of the log file for trace output

%s4 = Environment definition file name

Explanation

The path of the log file (%s3) for trace output could not be found.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the TraceLog directive that is set in the environment definition file (%s4).

8.5.3 ahs00403

AHS: ERROR: ahs00403: (%s1)%s2: Could not open TraceLog file %s3. [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Name of the log file for trace output

%s4 = Environment definition file name

Explanation

The log file (%s3) for trace output could not be opened.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check the TraceLog directive that is set in the environment definition file (%s4).

8.6 ahs00500 to ahs00599

This section details the messages numbered between ahs00500 and ahs00599.

8.6.1 ahs00500

AHS: ERROR: ahs00500: SSL: Library initialization failed.(%s1,%s2) [%s3]

Variable Information

%s1 = Error details context 1

%s2 = Error details context 2

%s3 = Environment definition file name

Explanation

Loading of a library required for SSL communication failed.

System Action

The web server start processing is canceled.

User Action

Install the following functions (packages).

Platform	Functions	Package name
Windows32/64	Secure Communication Service package	-
Solaris32	Interstage Secure Communication Service	FJSVisscs
	CA/EE common certificate management function, key management function	FJSVsmee
	Securecrypto Library RunTime	FJSVslcr
	Secure Socket Option	FSUNssl
Solaris64	Interstage Secure Communication Service	FJSVisscs
	CA/EE common certificate management function, key management function	FJSVsmee64
	Securecrypto Library RunTime	FJSVslcr64
Linux32	Interstage Secure Communication Service	FJSVsmee
	CA/EE common certificate management function, key management function	FJSVisscs
	Securecrypto Library RunTime	FJSVslcr
Linux64	Interstage Secure Communication Service	FJSVisscs
	CA/EE common certificate management function, key management function	FJSVsmee64
	Securecrypto Library RunTime	FJSVslcr64

If this error message continues to be displayed, collect diagnostic information using the *iscollectinfo* command, and then [contact your SE \(systems engineer\)](#).

8.6.2 ahs00501

AHS: ERROR: ahs00501: SSL: Insufficient memory.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The SSL library memory became insufficient.

System Action

The web server start processing is canceled.

User Action

Close any unnecessary programs, or check that sufficient memory is reserved for the web server operation.

8.6.3 ahs00502

AHS: ERROR: ahs00502: SSL: Slot information directory error.(%s1,%s2,%s3) [%s4]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = Environment definition file name

Explanation

There is an error in the slot information directory.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Check the settings of the [SSLSlotDir](#) directive in the environment definition file (%s4).
- Check the settings of the private key management environment.

8.6.4 ahs00503

AHS: ERROR: ahs00503: SSL: Invalid Token label.(%s1,%s2,%s3) [%s4]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = Environment definition file name

Explanation

The token label is incorrect.

System Action

The web server start processing is canceled.

User Action

Check that the token label matches the token label to which the site key certificate was registered.

8.6.5 ahs00504

AHS: ERROR: ahs00504: SSL: The site certificate has expired.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname.
- %s5 = Environment definition file name

Note

The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The site certificate has expired.

System Action

The web server execution processing is aborted.

User Action

Request the CA to issue a new site certificate, and reregister the new site certificate.

Point

The validity term of the site certificate can be checked by performing the following steps:

- For the Interstage certificate environment:
 1. In the Interstage Management Console, click [Security] > [Certificates] > [Site Certificate].
 2. Check [Validity Term] in the [Certificates: Site Certificate] page.
- For a certificate/key management environment configured with the SMEE command:

Check the validity term using the *cmdspcert* command.

8.6.6 ahs00505

AHS: ERROR: ahs00505: SSL: The CA certificate has expired.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name

Note

The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

One of the following causes is assumed:

- If this message is output when the web server starts, the certification authority (CA) certificate in the Interstage is expired.
- If this message is output during SSL communication with the client, the certification authority (CA) certificate in Interstage or the client (**Note**) has expired.

Note) Client authentication must have been performed in these cases

System Action

One of the following processing types will be performed:

- If this message is output when the web server starts, the web server start processing is canceled.
- If this message is output during SSL communication with the client, the communication with the client ends.

User Action

Take one of the following actions:

- If the certification authority (CA) certificate registered in Interstage has expired, obtain a new CA certificate from the CA, and reregister the new CA certificate in Interstage.
- If the certification authority (CA) certificate registered in the client has expired, obtain a new CA certificate from the CA, and reregister the new CA certificate in the client.

Point

The validity term of the CA certificate can be checked by performing the following steps:

- For the Interstage certificate environment:
 1. In the Interstage Management Console, click [Security] > [Certificates] > [CA Certificate].
 2. Check [Validity Term] in the [Certificates: CA Certificate] page.
- For a certificate/key management environment configured with the SMEE command:

Check the validity term using the *cmdspcert* command.

8.6.7 ahs00506

AHS: ERROR: ahs00506: SSL: Couldn't verify the site certificate.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name

Note

The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

Verification of the CA certificate and the site certificate failed.

System Action

The web server start processing is canceled.

User Action

Check that there is no error in the relationship between the CA certificate and the site certificate.

8.6.8 ahs00507

AHS: ERROR: ahs00507: SSL: Couldn't verify the CA certificate.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

Verification of the CA certificate failed.

System Action

The web server start processing is canceled.

User Action

Check that there is no error in the relationship between the CA certificate and the site certificate.

8.6.9 ahs00508

AHS: ERROR: ahs00508: SSL: Couldn't analyze the site certificate.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

Analysis of the site certificate failed.

System Action

The web server start processing is canceled.

User Action

Request the CA to issue a new site certificate, and reregister the newly issued site certificate.

8.6.10 ahs00509

AHS: ERROR: ahs00509: SSL: Couldn't analyze the CA certificate.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

Analysis of the CA certificate failed.

System Action

The web server start processing is canceled.

User Action

Obtain a new CA certificate from the CA, and reregister the obtained CA certificate.

8.6.11 ahs00510

AHS: ERROR: ahs00510: SSL: The site certificate has been revoked.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The site certificate has been revoked.

System Action

The web server start processing is canceled.

User Action

Request the CA to issue a new site certificate, and reregister the newly issued site certificate.

8.6.12 ahs00511

AHS: ERROR: ahs00511: SSL: The CA certificate has been revoked.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The CA certificate has been revoked.

System Action

The web server start processing is canceled.

User Action

Obtain a new CA certificate from the CA, and reregister the newly obtained CA certificate.

8.6.13 ahs00512

AHS: ERROR: ahs00512: SSL: Invalid Site certificate nickname.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The nickname of the site certificate is incorrect.

System Action

The web server start processing is canceled.

User Action

Check that the nickname of the site certificate specified in the [SSLCertName](#) directive in the environment definition file (%s5) is the same as the nickname that was registered in the certificate/key management environment using the *cmlistcert* command.

8.6.14 ahs00513

AHS: ERROR: ahs00513: SSL: Invalid Client CA certificate nickname.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

%s1 = Error issuer function name
%s2 = Error details context 1
%s3 = Error details context 2
%s4 = SSL definition name or site certificate nickname
%s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The nickname of the client CA certificate is incorrect.

System Action

The web server start processing is canceled.

User Action

Check that the nickname of the client CA certificate matches the one registered in the certificates and in the key management environment.

8.6.15 ahs00514

AHS: ERROR: ahs00514: SSL: The site certificate has no path list.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

%s1 = Error issuer function name
%s2 = Error details context 1
%s3 = Error details context 2
%s4 = SSL definition name or site certificate nickname
%s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The certificate pathway for the site certificate does not exist.

System Action

The web server start processing is canceled.

User Action

Register the CA certificate which issued the site certificate in the certificate/key management environment, starting with the root CA.

8.6.16 ahs00515

AHS: ERROR: ahs00515: SSL: The CA certificate has no path list.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The certificate pathway for the CA certificate does not exist.

System Action

The web server start processing is canceled.

User Action

Register the CA certificate in the certificates and in the key management environment sequentially from the root CA.

8.6.17 ahs00516

AHS: ERROR: ahs00516: SSL: The site certificate path is invalid.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The certificate pathway for the site certificate is incomplete.

System Action

The web server start processing is canceled.

User Action

Register the CA certificate which issued the site certificate in the certificate/key management environment, starting with the root CA.

8.6.18 ahs00517

AHS: ERROR: ahs00517: SSL: The CA certificate path is invalid.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or nickname of the site certificate
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The certificate pathway for the CA certificate is incomplete.

System Action

The web server start processing is canceled.

User Action

Register the CA certificate in the certificates and in the key management environment sequentially from the root CA.

8.6.19 ahs00518

AHS: ERROR: ahs00518: SSL: Private key does not exist.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

One of the following causes is assumed:

- The site private key is not registered in the private key management environment.
- A certificate in use was issued by an unsupported certificate authority.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Check that the site certificate was issued by the CSR created using the *scsmakeenv* or *cmmakecsr* commands on the server that uses the certificate.

- If a site certificate issued by Systemwalker PkiMGR is used, and the Site private key is not registered in the private key management environment, use the *cmenterkey* command to register the site private key in the private key management environment.
- If a certificate issued by an unsupported certificate authority is used, create a certificate signing request again, and submit it to the following certificate authorities to request the issuing of a certificate:
 - "Secure Site SSL Certificates" certificates issued by the VeriSign Inc.
 - "Secure Site with EV SSL Certificates" certificates and CRL issued by the VeriSign Inc.
 - "Cybertrust SureServer Certificate" and CRL issued by the Cybertrust, Inc.

8.6.20 ahs00519

AHS: ERROR: ahs00519: SSL: Invalid User pin.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

The user PIN is incorrect.

System Action

The web server start processing is canceled.

User Action

Reregister the user PIN.

8.6.21 ahs00520

AHS: ERROR: ahs00520: SSL: Certificate environment directory error.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

- %s1 = Error issuer function name
- %s2 = Error details context 1
- %s3 = Error details context 2
- %s4 = SSL definition name or site certificate nickname
- %s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

There is an error in the operation control directory.

System Action

The web server start processing is canceled.

User Action

Take one of the following actions:

- Check the settings of the [SSLEnvDir](#) directive in the environment definition file (%s5).
- Check the settings of the certificate and key management environment.

8.6.22 ahs00521

AHS: ERROR: ahs00521: SSL: Invalid cipher suite.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

%s1 = Error issuer function name

%s2 = Error details context 1

%s3 = Error details context 2

%s4 = SSL definition name or site certificate nickname

%s5 = Environment definition file name



Note

.....
The SSL definition name or site certificate nickname (%s4) may not be output.
.....

Explanation

The [SSLCipherSuite](#) directive has been specified incorrectly in the environment definition file (%s5).

System Action

The web server start processing is canceled.

User Action

Check that the method of encryption specified in the [SSLCipherSuite](#) directive in the environment definition file (%s5) can be specified.

8.6.23 ahs00522

AHS22: ERROR: ahs00522: SSL: SSL definition name specification is invalid.(%s1) [%s2]

Variable Information

%s1 = SSL definition name

%s2 = Environment definition file name

Explanation

The SSL definition (%s1) does not exist.

System Action

The web server start processing is canceled.

User Action

Check whether the Interstage certificate environment has been set up correctly.

If it has, specify the correct SSL definition name for the `SSLConfName` directive in the environment definition file (%s2).

8.6.24 ahs00523

AHS22: ERROR: ahs00523: SSL: SSL definition acquisition failed.(%s1,%s2,%s3) [%s4]

Variable Information

%s1 = SSL definition name

%s2 = Function name

%s3 = Error details context

%s4 = Environment definition file name

Explanation

SSL definition (%s1) certificate information failed to be acquired.

System Action

The web server start processing is canceled.

User Action

Collect diagnostic information using the `iscollectinfo` command, and [contact your SE \(systems engineer\)](#).

8.6.25 ahs00524

AHS: ERROR: ahs00524: SSL: SSLSlotDir is not defined. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The `SSLSlotDir` directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the `SSLSlotDir` directive in the environment definition file (%s1).

8.6.26 ahs00525

AHS: ERROR: ahs00525: SSL: SSLTokenLabel is not defined. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The `SSLTokenLabel` directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the [SSLTokenLabel](#) directive in the environment definition file (%s1).

8.6.27 ahs00526

AHS: ERROR: ahs00526: SSL: SSLUserPINFile is not defined. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The [SSLUserPINFile](#) directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the [SSLUserPINFile](#) directive in the environment definition file (%s1).

8.6.28 ahs00527

AHS: ERROR: ahs00527: SSL: SSLVerifyClient is not defined. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The [SSLVerifyClient](#) directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the [SSLVerifyClient](#) directive in the environment definition file (%s1).

8.6.29 ahs00528

AHS: ERROR: ahs00528: SSL: SSLEnvDir is not defined. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The [SSLEnvDir](#) directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the [SSLEnvDir](#) directive in the environment definition file (%s1).

8.6.30 ahs00529

AHS: ERROR: ahs00529: SSL: SSLCertName is not defined. [%s1]**Variable Information**

%s1 = Environment definition file name

Explanation

The [SSLCertName](#) directive has not been set in the environment definition file (%s1).

System Action

The web server start processing is canceled.

User Action

Set the [SSLCertName](#) directive in the environment definition file (%s1).

8.6.31 ahs00530

AHS: ERROR: ahs00530: SSL: User PIN decryption failed.(%s1,%s2) [%s3]**Variable Information**

%s1 = Error details context 1

%s2 = Error details context 2

%s3 = Environment definition file name

Explanation

The user PIN could not be decrypted.

System Action

The web server start processing is canceled.

User Action

Create the user PIN file again using the [ihsregistupin](#) command.

If this error message continues to be displayed, collect diagnostic information using the [iscollectinfo](#) command, and [contact your SE \(systems engineer\)](#).

8.6.32 ahs00531

AHS: ERROR: ahs00531: SSL: Couldn't open user pin file.(%s1) [%s2]**Variable Information**

%s1 = User PIN file name

%s2 = Environment definition file name

Explanation

The user PIN file (%s1) could not be opened.

System Action

The web server start processing is canceled.

User Action

Check whether the user PIN file (%s1) exists.

8.6.33 ahs00532

AHS: ERROR: ahs00532: SSL: Couldn't read user pin file.(%s1) [%s2]**Variable Information**

%s1 = User PIN file name

%s2 = Environment definition file name

Explanation

The user PIN file (%s1) could not be read.

System Action

The web server start processing is canceled.

User Action

Check the user PIN file (%s1) authority. If the authority has been set correctly, user PIN file (%s1) may be corrupt. Create the user PIN file again using the [ihsregistupin](#) command.

If this error message continues to be displayed, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.6.34 ahs00534

AHS: WARNING: ahs00534: SSL: The site certificate validity term has expired.(%s1,%s2) [%s3]**Variable Information**

%s1 = site certificate nickname

%s2 = site certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

%s3 = Environment definition file name

Explanation

The validity term (%s2) of the site certificate (%s1) has expired.

If a web server operation is continued even though the site certificate's validity term has already expired, the following problems will occur:

- Communication with the client fails.
- The web server cannot be restarted.

System Action

The web server execution processing is continued.

User Action

Take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new site certificate.
2. Reregister a new site certificate.
3. Restart the web server.

8.6.35 ahs00535

AHS: WARNING: ahs00535: SSL: The CA certificate validity term has expired.(%s1,%s2) [%s3]**Variable Information**

%s1 = CA certificate serial number

%s2 = CA certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

%s3 = Environment definition file name

Explanation

The validity term (%s2) of the CA certificate has expired.

If a web server operation is continued even though the CA certificate's validity term has already expired, the following problems will occur:

- Communication with the client fails.
- The web server cannot be restarted.

System Action

The web server execution processing is continued.

User Action

Take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new CA certificate.
2. Reregister a new CA certificate.
3. Restart the web server.

8.6.36 ahs00536

AHS: WARNING: ahs00536: SSL: The site certificate will expire in %s1 days.(%s2,%s3) [%s4]

Variable Information

%s1 = Number of days left until the site certificate's validity term will expire

%s2 = site certificate nickname

%s3 = site certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

%s4 = Environment definition file name

Explanation

The validity term (%s3) of the site certificate (%s2) will expire in %s1 days.

System Action

The web server execution processing is continued.

User Action

Before the validity term of the site certificate expires, take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new site certificate.
2. Reregister a new site certificate.
3. Restart the web server.

8.6.37 ahs00537

AHS: WARNING: ahs00537: SSL: The CA certificate will expire in %s1 days.(%s2,%s3) [%s4]

Variable Information

%s1 = Number of days left until the CA certificate's validity term will expire

%s2 = CA certificate serial number

%s3 = CA certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

%s4 = Environment definition file name

Explanation

The validity term (%s3) of the CA certificate will expire in %s1 days.

System Action

The web server execution processing is continued.

User Action

Before the validity term of the CA certificate expires, take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new CA certificate.
2. Reregister a new CA certificate.
3. Restart the web server.

8.6.38 ahs00538

AHS: ERROR: ahs00538: (%s1)%s2: SSL: Failed to generate the certificate monitoring daemon. func=%s3 [%s4]

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Function name

%s4 = Environment definition file name

Explanation

Failed to generate the certificate monitoring daemon.

System Action

The web server start processing is canceled.

User Action

Refer to the error details content (%s2), resolve the error, and then restart the web server.

8.6.39 ahs00539

AHS: ERROR: ahs00539: SSL: Not enough memory in the SCMI library. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The SCMI library memory became insufficient.

System Action

The web server start processing is canceled.

User Action

Check that there is sufficient memory. If there is insufficient memory, close unnecessary programs and secure the required memory capacity for running the web server.

8.6.40 ahs00540

AHS: ERROR: ahs00540: SSL: An error has occurred in the SCMI library function.(%s1,%s2) [%s3]

Variable Information

%s1 = SCMI library function name

%s2 = Additional information

%s3 = Environment definition file name

Explanation

An error occurred in the SCMI library function (%s1). The certificate/key management environment may be invalid.

System Action

The web server start processing is canceled.

User Action

Check whether the certificate/key management environment settings are valid. If the certificate/key management environment settings are valid, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.6.41 ahs00599

AHS: ERROR: ahs00599: SSL: Unexcepected error.(%s1,%s2,%s3,%s4) [%s5]

Variable Information

%s1 = Error issuer function name

%s2 = Error details context 1

%s3 = Error details context 2

%s4 = SSL definition name or site certificate nickname

%s5 = Environment definition file name



The SSL definition name or site certificate nickname (%s4) may not be output.

Explanation

An unexpected error was detected in the SSL function.

System Action

The web server start processing is canceled.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.7 ahs70000 to ahs70099

This section details the messages numbered between ahs70000 and ahs70099.

8.7.1 ahs70004

AHS: ERROR: ahs70004: (%s1)%s2:Cannot get enough memory

Variable Information

%s1 = Error details number

%s2 = Error details content

Explanation

Failed to acquire work memory.

User Action

Close unnecessary programs.

8.7.2 ahs70005

AHS: ERROR: ahs70005: (%s1)%s2:Error writing to log file. %s3 messages lost.

Variable Information

%s1 = Error details number

%s2 = Error details content

%s3 = Message management number in the log file (Internal code)

Explanation

Failed to write to the log file. There might not be enough space on the disk that stores the log files.

User Action

Make sure that there is enough space on the disk of the log file directory specified in the log rotation command ([ahsrlog](#)) in the environment definition file (httpd.conf).

If disk space is not the problem, remove the cause of error by referring to the error details content (%s2).

8.7.3 ahs70007

AHS: INFO: ahs70007: Log can now be output to the log file(%s1). (%s2)

Variable Information

%s1 = File name

%s2 = Number of messages failed to be output.

Explanation

Log can now be output to the log file (%s1).

8.7.4 ahs70008

AHS: INFO: ahs70008: The file was rotated because the file size of the log file(%s1) reached the upper limit of the system.

Variable Information

%s1 = File name

Explanation

The file was rotated because the file size of the log file (%s1), reached the system's upper limit.

8.7.5 ahs70009

AHS: ERROR: ahs70009: The log could not be output because the file size of the log file reached the upper limit of the system.

Explanation

The log could not be output because the log file size reached the system's upper limit.

System Action

The web server execution processing is aborted.

User Action

Stop the web server, back up the log file that reached the file size upper limit for the system, and then restart the web server.



Change the file size upper limit of the system using the *ulimit* command (for Bourne shell types) or the *limit* command (for C shell types). Restart the web server in the relevant shell to use the updated values.

8.8 ahs81000 to ahs81099

This section details the messages numbered between ahs81000 and ahs81099.

8.8.1 ahs81001

AHS: INFO: ahs81001: HTTP Server is starting. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server is starting.

8.8.2 ahs81002

AHS: INFO: ahs81002: HTTP Server is stopping. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server is stopping.

8.8.3 ahs81003

AHS: INFO: ahs81003: HTTP Server is restarting. [%s1]

Variable Information

%s1 = Environment definition file name

Explanation

The web server is restarting.

8.9 ahs81400 to ahs81499

This section details the messages numbered between ahs81400 and ahs81499.

8.9.1 ahs81400

AHS: ERROR: ahs81400: The file could not be opened. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = System call error number

%s3 = Error Details information

Explanation

The file (%s1) could not be opened.

System Action

The command returns an error.

User Action

Take the action described in table below, according to the file name (%s1).

File name (%s1)	Meaning/Required Action
Solaris32/64 Linux32/64 When the file name (%s1) begins with the socket file name (*1)	The web server may have been started. Stop the web server, and then reexecute the command.
All other cases	Refer to the system call error number (%s2), and remove the cause of the failure to open the file (%s1).

*1: This is the value set for the ScriptSock directive in the environment definition file (httpd.conf). The default value is "<value set for the ServerRoot directive>/logs/cgisock".

8.9.2 ahs81401

AHS: ERROR: ahs81401: The file could not be read. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = System call error number

%s3 = Error Details information

Explanation

The file (%s1) could not be read.

System Action

The command returns an error.

User Action

Refer to the error number (%s2), and remove the cause of the failure to read the file (%s1).

8.9.3 ahs81402

AHS: ERROR: ahs81402: The environment definition contains an error. %s1

Variable Information

%s1 = Error Details information

Explanation

The environment definition file contains an error.

System Action

The command returns an error.

User Action

Refer to the error details information (%s1) and check for syntax errors.

8.9.4 ahs81403

AHS: ERROR: ahs81403: Memory could not be obtained. func=%s1, errno=%s2, %s3

Variable Information

%s1 = Function name

%s2 = System call error number

%s3 = Error Details information

Explanation

Memory could not be obtained.

System Action

The command returns an error.

User Action

Terminate any unnecessary programs that have been activated.

8.9.5 ahs81404

AHS: INFO: ahs81404: The backup processing has commenced.

Explanation

The backup process has commenced.

8.9.6 ahs81405

AHS: INFO: ahs81405: The backup processing has been completed normally.

Explanation

The backup process has been completed normally.

8.9.7 ahs81406

AHS: ERROR: ahs81406: An error has been generated in the backup processing.

Explanation

An error was generated during the backup process.

System Action

The command returns an error.

User Action

Refer to the message output immediately before this message, and remove the cause of the error.

8.9.8 ahs81407

AHS: INFO: ahs81407: The restore processing has commenced.

Explanation

The restore process has commenced.

8.9.9 ahs81408

AHS: INFO: ahs81408: The restore processing has been completed normally.

Explanation

The restore process has been completed normally.

8.9.10 ahs81409

AHS: ERROR: ahs81409: An error has been generated in the restore processing.

Explanation

An error was generated during the restore process.

System Action

The command returns an error.

User Action

Refer to the message output immediately before this message, and remove the cause of the error.

8.9.11 ahs81410

**AHS: ERROR: ahs81410: The specification method of the option is incorrect.
Usage: ahsbackup -d directory [-t pass|all]**

Explanation

The specification method of the option in the `ahsbackup` command is incorrect.

System Action

The command returns an error.

User Action

Specify the option in the following syntax and reexecute the command.

```
ahsbackup -d directory [-t pass|all]
```

8.9.12 ahs81411

**AHS: ERROR: ahs81411: The specification method of the option is incorrect.
Usage: ahsrestore -d directory [-t pass|all] [-h host_table]**

Explanation

The specification method of the option in the [ahsrestore](#) command is incorrect.

System Action

The command returns an error.

User Action

Specify the option in the following syntax and reexecute the command.

```
ahsrestore -d directory [-t pass|all] [-h host_table]
```

8.9.13 ahs81412

AHS: ERROR: ahs81412: The user who executed the command does not have execution rights.

Explanation

The user who executed the command does not have execution rights.

System Action

The command returns an error.

User Action

Reexecute the command with Administrator rights.

8.9.14 ahs81413

AHS: ERROR: ahs81413: The environment definition file cannot be located. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The environment definition file (%s1) cannot be located.

System Action

The command returns an error.

User Action

Locate the environment definition file (%s1) and reexecute the command.

8.9.15 ahs81414

AHS: ERROR: ahs81414: The specified storage directory cannot be located. dir=%s1, errno=%s2, %s3

Variable Information

%s1 = Directory name

%s2 = Error detail number

%s3 = Error details content

Explanation

The storage directory (%s1) specified in the -d option cannot be located.

System Action

The command returns an error.

User Action

Specify the correct storage directory in the -d option, and reexecute the command.

8.9.16 ahs81415

AHS: ERROR: ahs81415: The path name of the directory to be created is too long. dir=%s1

Variable Information

%s1 = Directory name

Explanation

The path name of the directory to be created is too long. The work directory (%s1) could not be created during the backup/export process under the storage directory because the directory path name was too long.

System Action

The command returns an error.

User Action

Shorten the path name of the storage directory specified in the -d option and reexecute the command.

8.9.17 ahs81416

AHS: ERROR: ahs81416: The directory could not be created. dir=%s1, errno=%s2, %s3

Variable Information

%s1 = Directory name

%s2 = Error detail number

%s3 = Error details content

Explanation

The directory (%s1) could not be created.

System Action

The command returns an error.

User Action

Refer to the error details content (%s3), and remove the cause of the error.

8.9.18 ahs81417

AHS: ERROR: ahs81417: The backup resource management file cannot be located. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The backup resource management file (%s1) cannot be located.

System Action

The command returns an error.

User Action

Specify the directory containing the backup resource management file (%s1) in the -d option and reexecute the command.

8.9.19 ahs81418

AHS: ERROR: ahs81418: Information on the backup resource management file has been destroyed. %s1

Variable Information

%s1 = Error details information

Explanation

Information on the backup resource management file (*ahs_info.ahs*) has been destroyed.

System Action

The command returns an error.

User Action

Collect the backup resource file (*ahs_info.ahs*) and diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.9.20 ahs81419

AHS: ERROR: ahs81419: The backup resource management file could not be created. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The backup resource management file (%s1) could not be created. The path name of the backup resource management file may be too long.

System Action

The command returns an error.

User Action

Shorten the path name of the storage directory specified in the -d option and reexecute the command.

If the message continues to be output, refer to the error details content (%s3), and remove the cause of the error.

8.9.21 ahs81420

AHS: ERROR: ahs81420: The backup resource management file could not be written to. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The backup resource management file (%s1) could not be written to.

System Action

The command returns an error.

User Action

Refer to the error details content (%s3), and remove the cause of the error.

8.9.22 ahs81421

AHS: ERROR: ahs81421: The type of the destination drive for copying is not supported. drive=%s1, type=%s2

Variable Information

%s1 = Drive name

%s2 = Drive type

Explanation

The type (%s2) of the destination drive (%s1) for copying is not supported in the resource restore/import process.

System Action

The command returns an error.

User Action

Allocate the drive specified in the drive name (%s1) to the system's fixed drive, network drive, or REMOVABLE drive and reexecute the command.

8.9.23 ahs81422

AHS: ERROR: ahs81422: The original file for copying cannot be located. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The original file (%s1) for copying could not be located during the resource restore/import process.

System Action

The command returns an error.

User Action

If the file specified in the file name (%s1) was deleted, locate the file manually and reexecute the command.

8.9.24 ahs81423

AHS: ERROR: ahs81423: The required drive cannot be located at the destination for copying. drive=%s1

Variable Information

%s1 = Drive name

Explanation

The drive (%s1) required for the resource restore/import process cannot be located.

System Action

The command returns an error.

User Action

Create the drive specified in the drive name (%s1) in the system and reexecute the command.

8.9.25 ahs81424

AHS: ERROR: ahs81424: The file could not be copied. from=%s1, to=%s2, errno=%s3, %s4

Variable Information

%s1 = Name of the original file for copying

%s2 = Name of the destination file for copying

%s3 = Error detail number

%s4 = Error details content

Explanation

The file could not be copied. The destination disk for copying may be full.

System Action

The command returns an error.

User Action

Check that there is sufficient space in the destination disk for copying. Allocate sufficient space and reexecute the command.

If the message continues to be output, refer to the error details content (%s4), and remove the cause of the error.

8.9.26 ahs81425

AHS: ERROR: ahs81425: Specification of the resource storage directory contains an error. dir=%s1

Variable Information

%s1 = Directory name

Explanation

The error may be caused by one of the following:

- The resource storage directory (%s1) specified in the -d option contains an error.
- Files required for restore/import processing in the following directories in the resource storage directory (%s1) specified in the -d option do not exist.
 - Windows32/64
AHS

- [Solaris32/64](#) [Linux32/64](#)
FJSVahs

System Action

The command returns an error.

User Action

Take one of the following actions:

- [Solaris32/64](#) [Linux32/64](#)

Ensure the directory specified in the -d option does not contain the following errors:

- A relative path has been specified.
- A directory immediately below the root directory has been specified.

Specify the correct absolute path and reexecute the command.

- If there are no files in the directory (%s1) which was specified in the -d option, perform the backup and export processing again, and then reexecute the restore and import process.

8.9.27 ahs81426

AHS: ERROR: ahs81426: The resource storage directory could not be created. dir=%s1, errno=%s2, %s3

Variable Information

- %s1 = Directory name
- %s2 = Error detail number
- %s3 = Error details content

Explanation

The resource storage directory (%s1) could not be created.

System Action

The command returns an error.

User Action

Move the resource storage directory to a disk with sufficient space and reexecute the command.

If the message continues to be output, refer to the error details content (%s3), and remove the cause of the error.

8.9.28 ahs81427

AHS: ERROR: ahs81427: The resource storage directory has already been located. dir=%s1

Variable Information

- %s1 = Directory name

Explanation

The following directory is already located under the directory specified in the -d option.

- [Windows32/64](#)
AHS
- [Solaris32/64](#) [Linux32/64](#)
FJSVahs

System Action

The command returns an error.

User Action

The above directory is automatically created under the directory specified in the -d option during the resource backup process.

If the above directory is not required, delete it and reexecute the command.

If the above directory is required, move it to a storage medium, or change the directory specified in the -d option and reexecute the command

8.9.29 ahs81428

AHS: ERROR: ahs81428: The directory under the resource storage directory cannot be located. dir=%s1, errno=%s2, %s3

Variable Information

%s1 = Directory name

%s2 = Error detail number

%s3 = Error details content

Explanation

The following directory is not located under the directory specified in the -d option.

- **Windows32/64**
AHS
- **Solaris32/64 Linux32/64**
FJSVahs

System Action

The command returns an error.

User Action

Specify the upper directory in the -d option and reexecute the command.

8.9.30 ahs81429

AHS: ERROR: ahs81429: The saved resource could not be deleted due to a backup processing error. func=%s1, errno=%s2, %s3

Variable Information

%s1 = Function name

%s2 = Error detail number

%s3 = Error details content

Explanation

An attempt was made to delete the saved resource due to a resource backup/export processing error, but an error occurred during the delete.

System Action

The command returns an error.

User Action

The following directory has remained under the directory specified in the -d option. Delete the following directory and all sub directories.

- **Windows32/64**
AHS
- **Solaris32/64** **Linux32/64**
FJSVahs

8.9.31 ahs81430

AHS: ERROR: ahs81430: An internal error has been generated. %s1

Variable Information

%s1 = Error details information

Explanation

An internal error has been generated.

System Action

The command returns an error.

User Action

Refer to the error details information (%s1), and remove the cause of the error.

If the message continues to be output, collect diagnostic information with the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.9.32 ahs81431

AHS: ERROR: ahs81431: Specification in the host convertible file contains an error. %s1

Variable Information

%s1 = Error details information

Explanation

There is an error in the specification of the host convertible file in the -h option.

System Action

The command returns an error.

User Action

Refer to the error details information (%s1), and review the specification of the host convertible file.

8.9.33 ahs81432

AHS: ERROR: ahs81432: The environment definition temporary file could not be written to. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The environment definition temporary file (%s1) could not be written to.

System Action

The command returns an error.

User Action

Refer to the error details content (%s3), and remove the cause of the error.

8.9.34 ahs81433

AHS: ERROR: ahs81433: The name of the environment definition temporary file could not be changed. file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = Error detail number

%s3 = Error details content

Explanation

The name of the environment definition temporary file (%s1) could not be changed.

System Action

The command returns an error.

User Action

Refer to the error details content (%s3), and remove the cause of the error.

8.9.35 ahs81434

AHS: ERROR: ahs81434: ahsbackup or ahsrestore is already executing.

Explanation

The [ahsbackup](#) or [ahsrestore](#) command has already been executed by another process, and therefore, cannot be executed now.

System Action

The command returns an error.

User Action

After the execution of the [ahsbackup](#) or [ahsrestore](#) command terminates, reexecute the command.

8.9.36 ahs81435

AHS: ERROR: ahs81435: Processing cannot be performed because the Web server configuration is different.

Explanation

The restore or import conditions are not met, therefore processing cannot be performed.

System Action

The command returns an error.

User Action

Perform restore or import again in the state where one of the following conditions is met:

- Only the default web server exists
- All the following match in the backup, import source and restore, and import destination operating environments:
 - Number of web servers
 - Name of each web server (*1)
 - Path of the environment definition file for each web server (*1) (*2)

*1: Solaris32/64 Linux32/64

The uppercase and lowercase letters must match.

*2: Windows32/64

The environment definition file (httpd.conf) paths (including, 8.3 formats (short names)) set in the web server list file (servers.conf) must also match.

8.9.37 ahs81439

AHS: ERROR: ahs81439: Failed to write the file. : file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = System call error number

%s3 = Error details content

Explanation

The file (%s1) could not be written.

System Action

The command returns an error.

User Action

Refer to the error number (%s2), resolve the cause of the failure to write to the file (%s1), and then reexecute the command.

8.9.38 ahs81440

AHS: ERROR: ahs81440: Failed to close the file. : file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = System call error number

%s3 = Error details content

Explanation

The file (%s1) could not be closed.

System Action

The command returns an error.

User Action

Refer to the error number (%s2), resolve the cause of the failure to close the file (%s1), and then reexecute the command.

8.9.39 ahs81451

AHS: ERROR: ahs81451: Failed to delete the file. : file=%s1, errno=%s2, %s3

Variable Information

%s1 = File name

%s2 = System call error number

%s3 = Error details content

Explanation

The file (%s1) could not be deleted.

System Action

The command returns an error.

User Action

Refer to the error number (%s2), resolve the cause of the failure to delete the file (%s1), and then reexecute the command.

8.9.40 ahs81452

AHS: ERROR: ahs81452: Processing cannot be performed because the install information of the service is different. Service name:%s1

Variable Information

%s1 = Service name

Explanation

The environment definition file path specified when the service (%s1) was registered may be different than the service with the same name in the backup, import source and restore, and import destination operating environments.

System Action

Stops command processing.

User Action

Delete the service (%s1) from the restore and import destination operating environments, and then perform the restore and import again.

8.9.41 ahs81453

AHS: ERROR: ahs81453: The Web server cannot be restored because the service is running. Service name:%s1

Variable Information

%s1 = Service name

Explanation

The web server cannot be restored because the service (%s1) is running.

System Action

Stops command processing.

User Action

Stop the service (%s1) and repeat the restore process.

8.10 Error Log

Interstage HTTP Server 2.2 error messages are output to error log files as follows (default setting):

Output Directory

Error logs are generated in the following directory:

Windows32/64 (The installation path is the default path.)

```
C:\Interstage\F3FMahs\logs\errorlog
```

Solaris32/64 (The installation path is the default path.) **Linux32/64**

```
/var/opt/FJSVahs/logs/errorlog
```

Output Timing

The error log is output when an error occurs in the web server.

Output Format

The output format of an error log is as follows:

```
[Date-and-Time] [Log-level] [client IP-address] (Error-number) Error-explanation: Message-body
```

Output Items

The details of each output item are as follows:

Date-and-Time

Indicates the date and time at which the error occurred.

Log-level

Table 8.1 Table 0-1 Log Levels

Log level	Severity of the error	Output with the default settings
emerg	Emergency error	The error is output.
alert	Fatal error that must be resolved immediately	The error is output.
crit	Error that must be resolved immediately	The error is output.
error	Insignificant error, ignorable	The error is output.
warn	Warning for an ignorable error	The error is output.
notice	Common event to be specially reported	The error is output.
info	Event not reported by notice (output only when the environment definition is modified)	The error is not output.
debug	Event logged during development or debug of a module (output only when the environment definition is modified)	The error is not output.

client IP-address

IP address of systems such as client or proxy server.

This item is output only when an error occurred on the client during access to Interstage HTTP Server 2.2. This item may be omitted.

Error-number

Indicates the number of an error as assigned in the operating system.

This item may be omitted.

Error-explanation

Brief description of an error.

This item may be omitted.

Message-body

Body of an error message.

The meaning and user action for each log level is explained in this chapter.

8.10.1 Messages Whose Log Levels are "emerg"

The meaning and user action for log level "emerg" is explained.

Message list

1. (%s1)%s2: %s3 failed. Attempting to shutdown process gracefully.
2. (%s1)%s2: apr_socket_accept: giving up.
3. (%s1)%s2: Couldn't create accept lock
4. (%s1)%s2: Couldn't initialize cross-process lock in child
5. (%s1)%s2: Couldn't initialize signal thread
6. (%s1)%s2: Couldn't set permissions on cross-process lock; check User and Group directives
7. (%s1)%s2: OpenEvent on %s3 event
8. (%s1)%s2: SetEvent on %s3 event

Explanation and User action of Messages

(%s1)%s2: %s3 failed. Attempting to shutdown process gracefully.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Function name

Explanation

An error has occurred in the communication process.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_socket_accept: giving up.**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

A network error was detected.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Couldn't create accept lock**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Exclusive resources for connection could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Couldn't initialize cross-process lock in child**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Exclusive resources for connection could not be initialized.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Couldn't initialize signal thread**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to initialize the signal in the thread.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Couldn't set permissions on cross-process lock; check User and Group directives

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Authority failed to be set for exclusive resources for connection.

System Action

The web server start processing is canceled.

User Action

Check the following directive in the environment definition file (httpd.conf).

- User
- Group

(%s1)%s2: OpenEvent on %s3 event

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

Explanation

Event object (%s3) could not be opened.

System Action

Web server execution processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

(%s1)%s2: SetEvent on %s3 event

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event object name

Explanation

The signal status for event object (%s3) could not be set.

System Action

Web server execution processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

8.10.2 Messages Whose Log Levels are "alert"

The meaning and user action for log level "alert" is explained.

Message list

1. %s1: Could not reliably determine the server's fully qualified domain name, using %s2 for ServerName
2. (%s1)%s2: ap_queue_info_create() failed
3. (%s1)%s2: ap_queue_init() failed
4. (%s1)%s2: apr_thread_create: unable to create listener thread
5. (%s1)%s2: apr_thread_create: unable to create worker thread
6. (%s1)%s2: Cannot chroot when not started as root
7. (%s1)%s2: Can't chdir to %s3
8. (%s1)%s2: Can't chdir to new root
9. (%s1)%s2: Can't chroot to %s3
10. (%s1)%s2: getpwuid: couldn't determine user name from uid %s3, you probably need to modify the User directive
11. (%s1)%s2: initgroups: unable to set groups for User %s3 and Group %s4
12. (%s1)%s2: malloc: out of memory
13. (%s1)%s2: mod_unique_id: unable to find hostname of the server
14. (%s1)%s2: mod_unique_id: unable to find IPv4 address of "%s3"
15. (%s1)%s2: set_dumpable failed - this child will not coredump after software errors
16. (%s1)%s2: setgid: unable to set group id to Group %s3
17. (%s1)%s2: setuid: unable to change to uid: %s3
18. Child %s1 returned a Fatal error... Apache is exiting!
19. No active workers found... Apache is exiting!
20. no listening sockets available, shutting down
21. refusing to send signal %s1 to pid %s2 outside process group

Explanation and User action of Messages

%s1: Could not reliably determine the server's fully qualified domain name, using %s2 for ServerName

Variable Information

%s1 = Web server execution program name

%s2 = Host name or IP address

Explanation

The fully qualified domain name (FQDN) could not be detected.

System Action

The web server start processing is continued.

User Action

Check the ServerName directive in the environment definition file (httpd.conf). If the ServerName directive has been set correctly, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

(%s1)%s2: ap_queue_info_create() failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to create the internal queue.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ap_queue_init() failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to initialize the internal queue.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_thread_create: unable to create listener thread

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to generate the listener thread.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_thread_create: unable to create worker thread

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The communication thread could not be created.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Cannot chroot when not started as root

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Unable to retrieve the daemon process start user ID.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Can't chdir to %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Directory name

Explanation

Unable to change the current directory to the directory (%s3).

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Check the ChrootDir directive in the environment definition file (httpd.conf).

(%s1)%s2: Can't chdir to new root

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Unable to change the current directory.

System Action

The web server start processing is canceled.

User Action

Check the ChrootDir directive in the environment definition file (httpd.conf).

(%s1)%s2: Can't chroot to %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Directory name

Explanation

Unable to change the root directory to the directory (%s3).

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: getpwuid: couldn't determine user name from uid %s3, you probably need to modify the User directive

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID



The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.

Explanation

The User ID (%s3) entry specified for the User directive in the environment definition file (httpd.conf) could not be obtained.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check User ID specified by the User directive in the environment definition file (httpd.conf).

(%s1)%s2: initgroups: unable to set groups for User %s3 and Group %s4

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID

%s4 = Group ID

Explanation

The group access list could not be initialized.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: malloc: out of memory

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Memory could not be obtained.

System Action

The web server program execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: mod_unique_id: unable to find hostname of the server

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The host name could not be acquired.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: mod_unique_id: unable to find IPv4 address of "%s3"

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

Explanation

The name of Host (%s3) could not be resolved.

System Action

Windows32/64

Web server execution processing is continued.

Solaris32/64 **Linux32/64**

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: set_dumpable failed - this child will not coredump after software errors

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The core dump could not be set.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: setgid: unable to set group id to Group %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Group ID

Explanation

The Group ID (%s3) specified for the Group directive in the environment definition file (httpd.conf) could not be set.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check Group ID specified by the Group directive in the environment definition file (httpd.conf).

(%s1)%s2: setuid: unable to change to uid: %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = User ID

Explanation

The User ID (%s3) specified for the User directive in the environment definition file (httpd.conf) could not be set.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Take one of the following actions:

- Resolve the cause of the error according to the error details context (%s2).
- Check User ID (%s3) specified by the User directive in the environment definition file (httpd.conf).

Child %s1 returned a Fatal error... Apache is exiting!

Variable Information

%s1 = Process ID of the communication process

Explanation

An error occurred in Process ID (%s1).

System Action

Web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

No active workers found... Apache is exiting!

Explanation

There are no active communication threads.

System Action

Web server execution processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

no listening sockets available, shutting down

Explanation

A valid Listen directive has not been set in the environment definition file (httpd.conf).

System Action

Web server execution processing is aborted.

User Action

If the Listen directive has not been set in the environment definition file (httpd.conf), set it. If the Listen directive has been set, refer to the message that was output at the same time and fix the error.

refusing to send signal %s1 to pid %s2 outside process group

Variable Information

%s1 = Signal type

%s2 = Process ID of the communication process

Explanation

This is a different process group, therefore the communication process (%s2) cannot send the signal (%s1).

System Action

Web server execution processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

8.10.3 Messages Whose Log Levels are "crit"

The meaning and user action for log level "crit" is explained.

Message list

1. (%s1)%s2: %s3: Failed to start the service process.
2. (%s1)%s2: %s3: Unable to start the service manager.
3. (%s1)%s2: alloc_listener: failed to get a socket for %s3
4. (%s1)%s2: alloc_listener: failed to set up sockaddr for %s3
5. (%s1)%s2: ap_queue_pop failed
6. (%s1)%s2: ap_queue_push failed
7. (%s1)%s2: apr_proc_detach failed
8. (%s1)%s2: apr_thread_join: unable to join %s3
9. (%s1)%s2: cannot allocate scoreboard
10. (%s1)%s2: Child %s3: _beginthreadex failed. Unable to create all worker threads. Created %s4 of the %s5 threads requested with the ThreadsPerChild configuration directive.
11. (%s1)%s2: Child %s3: Failed to create a %s4 event.

12. (%s1)%s2: Child %s3: setup_inherited_listeners(), WSASocket failed to open the inherited socket.
13. (%s1)%s2: Child %s3: Unable to access the scoreboard from the parent
14. (%s1)%s2: Child %s3: Unable to access the start_mutex from the parent
15. (%s1)%s2: Child %s3: Unable to reopen the scoreboard from the parent
16. (%s1)%s2: Child %s3: Unable to retrieve the exit event from the parent
17. (%s1)%s2: Child %s3: Unable to retrieve the ready event from the parent
18. (%s1)%s2: Child %s3: Unable to retrieve the scoreboard from the parent
19. (%s1)%s2: Child %s3: Unable to retrieve the start_mutex from the parent
20. (%s1)%s2: Child %s3: WAIT_FAILED -- shutting down server
21. (%s1)%s2: Could not open pipe-of-death.
22. (%s1)%s2: Failed to get the full path of %s3
23. (%s1)%s2: Fatal error: Invalid Scoreboard path %s3
24. (%s1)%s2: Fatal error: unable to create global pool for use with by the scoreboard
25. (%s1)%s2: Invalid -E error log file %s3
26. (%s1)%s2: Invalid config file path %s3
27. (%s1)%s2: Invalid PID file path %s3, ignoring.
28. (%s1)%s2: make_sock: could not bind to address %s3
29. (%s1)%s2: make_sock: for address %s3, apr_socket_opt_set: (%s4)
30. (%s1)%s2: master_main: create child process failed. Exiting.
31. (%s1)%s2: master_main: WaitForMultipleObjects WAIT_FAILED -- doing server shutdown
32. (%s1)%s2: mod_rewrite: Parent could not create RewriteLock file %s3
33. (%s1)%s2: mod_rewrite: Parent could not set permissions on RewriteLock; check User and Group directives
34. (%s1)%s2: Parent: Cannot create %s3 event %s4
35. (%s1)%s2: Parent: Could not create %s3 event for child process
36. (%s1)%s2: Parent: Failed to create the child process.
37. (%s1)%s2: Parent: Failed to get full path of %s3
38. (%s1)%s2: Parent: Failed to get the current path
39. (%s1)%s2: Parent: Unable to create child stdin pipe.
40. (%s1)%s2: Parent: Unable to duplicate the %s3 handle for the child
41. (%s1)%s2: Parent: Unable to duplicate the start mutex to the child
42. (%s1)%s2: Parent: Unable to retrieve the %s3 for the child
43. (%s1)%s2: Parent: Unable to send the %s3 to the child
44. (%s1)%s2: Parent: Unable to write duplicated socket %s3 to the child.
45. (%s1)%s2: Parent: WSADuplicateSocket failed for socket %s3. Check the FAQ.
46. (%s1)%s2: read: rfc1413: error reading response
47. (%s1)%s2: rfc1413: apr_sockaddr_info_get(%s3) failed
48. (%s1)%s2: rfc1413: Error binding query socket to local port
49. (%s1)%s2: rfc1413: error creating query socket

50. (%s1)%s2: rfc1413: error setting query socket timeout
51. (%s1)%s2: setup_inherited_listeners: Unable to read socket data from parent
52. (%s1)%s2: unable to create or access scoreboard "%s3" (name-based shared memory failure)
53. (%s1)%s2: Unable to create or access scoreboard (anonymous shared memory failure)
54. (%s1)%s2: unable to replace stderr with %s3
55. (%s1)%s2: write: rfc1413: error sending request
56. [%s1] file %s2, line %s3, assertion "%s4" failed
57. [client %s1] (%s2)%s3: %s4 pcfg_openfile: unable to check htaccess file, ensure it is readable
58. [client %s1] configuration error: couldn't %s2: %s3
59. Fatal error: shared scoreboard too small for child!
60. Parent: child process exited with status %s1 -- Aborting.

Explanation and User action of Messages

(%s1)%s2: %s3: Failed to start the service process.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service (%s3) could not be started.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

(%s1)%s2: %s3: Unable to start the service manager.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The service control manager could not be started.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: alloc_listener: failed to get a socket for %s3**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

Explanation

The communication socket could not be created.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: alloc_listener: failed to set up sockaddr for %s3**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

Explanation

The Host (%s3) information specified for the Listen directive in the environment definition file (httpd.conf) could not be obtained.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ap_queue_pop failed**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to retrieve the request from the internal queue.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ap_queue_push failed**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to queue the received requests in the internal queue.

System Action

The requests are discarded, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_proc_detach failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

A daemon process could not be generated.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_thread_join: unable to join %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Thread name

Explanation

Failed to wait for the thread (%s3) to complete.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: cannot allocate scoreboard

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The dynamic memory that is used in the scoreboard could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: _beginthreadex failed. Unable to create all worker threads. Created %s4 of the %s5 threads requested with the ThreadsPerChild configuration directive.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID of the daemon process

%s4 = The number of communication threads that have been created

%s5 = The value set for the ThreadsPerChild directive

Explanation

The communication thread could not be created.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Failed to create a %s4 event.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

%s4 = Event name

Explanation

The event (%s4) could not be created.

System Action

The web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: setup_inherited_listeners(), WSASocket failed to open the inherited socket.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The communication socket could not be created.

System Action

The daemon process is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to access the scoreboard from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process failed to access the handle used for the scoreboard.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to access the start_mutex from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process failed to access the handle that controls exclusive use.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to reopen the scoreboard from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process failed to open the scoreboard.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to retrieve the exit event from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process could not retrieve the completion event handle from the start process.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to retrieve the ready event from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process could not retrieve the start event handle from the start process.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to retrieve the scoreboard from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The daemon process could not retrieve the handle, which is used for the scoreboard, from the start process.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Unable to retrieve the start_mutex from the parent

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

The communication process could not retrieve the handle, which controls exclusive use, from the daemon process.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: WAIT_FAILED -- shutting down server

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID

Explanation

An error occurred during wait processing.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Could not open pipe-of-death.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

A pipe could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to get the full path of %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Web server program name

Explanation

The full path of the web server program (%s3) could not be found.

System Action

Web server program execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Fatal error: Invalid Scoreboard path %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Scoreboard file path

Explanation

The path (%s3) of the scoreboard file could not be found.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Fatal error: unable to create global pool for use with by the scoreboard

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The memory management area that is used in scoreboard management could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Invalid -E error log file %s3**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = File name

Explanation

The error log file path is incorrect.

System Action

Web server program execution processing is aborted.

User Action

Check the name of the error log file that was specified using the -E option.

(%s1)%s2: Invalid config file path %s3**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Environment definition file

Explanation

The specified environment definition file (httpd.conf) path (%s3) is incorrect.

System Action

Web server execution processing is aborted.

User Action

Check the path of the specified environment definition file (httpd.conf).

(%s1)%s2: Invalid PID file path %s3, ignoring.**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Process management file name

Explanation

The path (%s3) of the process management file could not be found.

System Action

The web server start processing is continued.

User Action

Check the process management file specified by the PidFile directive in the environment definition file (httpd.conf).

If the PidFile directive has been set correctly, resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: make_sock: could not bind to address %s3**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

Explanation

An address could not be assigned to the socket.

System Action

The web server start processing is canceled.

User Action

Take the action described in table below, according to Error details number (%s1).

Error details number (%s1)	Meaning/Required Action
Windows32/64 OS 10013 OS 10048	If this message is output when the web server starts, take one of the following actions: If the web server was restarted immediately after being stopped, the release processing for the IP address or the port number (%s3) used by the web server that was stopped may not have completed. Wait for a while (several seconds), and then restart the web server. Another service is using the IP address and port number (%s3) or port number (%s3). Check whether the IP address and port number specified for the web server is also specified for another service. If so, terminate that service, or use a different IP address and/or port number. If the IP address and port number settings are correct, collect diagnostic information with the <i>iscollectinfo</i> command, and contact your SE (systems engineer) . If more than one Listen directive with the same IP address and port number combination has been set in the environment definition file (httpd.conf), delete the one that is not needed.
Solaris32/64 125	
Linux32/64 98	
Windows32/64 OS 10049	An invalid address was specified. Check the settings of the Listen directive in the environment definition file (httpd.conf).
Solaris32/64 126	
Linux32/64 22 99	
Linux32/64 99	The IP address (%3) was mapped to an invalid network interface. Check the settings of the network interface to which the IP address (%3) was mapped. If the settings are correct, collect diagnostic information with the <i>iscollectinfo</i> command, and contact your SE (systems engineer) .
All other cases	Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: make_sock: for address %s3, apr_socket_opt_set: (%s4)**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

%s4 = Socket option

Explanation

The socket option (%s4) could not be set.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: master_main: create child process failed. Exiting.

Variable Information

%s1 = Error details number

%s2 = Error details context



The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.

Explanation

The daemon process could not be created.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

(%s1)%s2: master_main: WaitForMultipleObjects WAIT_FAILED -- doing server shutdown

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

An error occurred in daemon process status monitoring.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: mod_rewrite: Parent could not create RewriteLock file %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Name of the lock file for the rewrite function

Explanation

The lock file (%s3) for the rewrite function could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: mod_rewrite: Parent could not set permissions on RewriteLock; check User and Group directives

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to set permissions for the lock file used for the rewrite feature.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Cannot create %s3 event %s4

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event name

%s4 = Object name

Explanation

The object (%s4) of the event (%s3) could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Could not create %s3 event for child process

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event name

Explanation

The object of the event (%s3) could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Failed to create the child process.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The daemon process could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Failed to get full path of %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Web server program name

Explanation

The path of the web server program (%s3) could not be obtained.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Failed to get the current path

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The current path could not be found.

System Action

The web server start processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to create child stdin pipe.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The pipe could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to duplicate the %s3 handle for the child

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event name

Explanation

Failed to copy the handle of the event (%s3).

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to duplicate the start mutex to the child

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to copy the handle that controls exclusive use.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to retrieve the %s3 for the child

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event name

Explanation

Failed to retrieve the handle of the event (%s3).

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to send the %s3 to the child

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Event name

Explanation

Failed to send the handle of the event (%s3).

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Unable to write duplicated socket %s3 to the child.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The start process failed to write the socket to the daemon process.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: WSADuplicateSocket failed for socket %s3. Check the FAQ.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Socket descriptor

Explanation

The socket could not be duplicated.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: read: rfc1413: error reading response

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Response reception from the socket failed in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: rfc1413: apr_sockaddr_info_get(%s3) failed

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address of the client

Explanation

Socket information could not be found in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: rfc1413: Error binding query socket to local port

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The socket could not be allocated in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: rfc1413: error creating query socket

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

A socket could not be created in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: rfc1413: error setting query socket timeout

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The socket timeout could not be set in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: setup_inherited_listeners: Unable to read socket data from parent

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Socket information from the start process could not be read.

System Action

The daemon process is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: unable to create or access scoreboard "%s3" (name-based shared memory failure)

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Scoreboard name

Explanation

The shared memory that is used in the scoreboard (%s3) could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Unable to create or access scoreboard (anonymous shared memory failure)

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The shared memory that is used in the scoreboard could not be acquired.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: unable to replace stderr with %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Output destination

Explanation

Unable to change the standard error output to the output destination (%s3).

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

[%s1]%s2: write: rfc1413: error sending request

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

There was a failure in the transmission request to the socket in the RFC1413 user identifier search.

System Action

User identifier information get processing is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

[%s1] file %s2, line %s3, assertion "%s4" failed

Variable Information

%s1 = Time of occurrence

%s2 = Source file name

%s3 = Source file line number

%s4 = Detailed information

Explanation

An error occurred in the web server.

System Action

Web server execution processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

[client %s1] (%s2)%s3: %s4 pcfg_openfile: unable to check htaccess file, ensure it is readable

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = Access control definition file name

Explanation

The access control definition file (%s3) could not be read.

System Action

A response is given using status code "403" (Forbidden).

User Action

Resolve the cause of the error according to the error details context (%s2).

[client %s1] configuration error: couldn't %s2: %s3

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Phase in which the internal error occurred

%s3 = Request URI

Explanation

Request processing could not be performed because an internal error occurred.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

Fatal error: shared scoreboard too small for child!

Explanation

The scoreboard could not be opened because the shared memory that is used in the scoreboard is too small.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

Parent: child process exited with status %s1 -- Aborting.

Variable Information

%s1 = Daemon process exit code

Explanation

An error occurred in the daemon process.

System Action

Web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

8.10.4 Messages Whose Log Levels are "error"

The meaning and user action for log level "error" is explained.



Note

Messages output by the CGI program to the standard error output use the format below (this message is not in "Message list" and "Explanation and User action of Messages", therefore take action according to the CGI program specification):

[client %s1] %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Message output by the CGI program to the standard error output

Message list

1. %s1: could not log pid to file %s2
2. %s1: Service is already installed.
3. %s1 not supported on this platform
4. (%s1)%s2: %s3: Failed to delete the service.
5. (%s1)%s2: %s3: Failed to open the service.
6. (%s1)%s2: %s3: Failed to store the ConfigArgs in the registry.
7. (%s1)%s2: %s3: getrlimit failed
8. (%s1)%s2: %s3: OpenService failed
9. (%s1)%s2: %s3: Unable to create the start_mutex.
10. (%s1)%s2: %s3: Unable to start the service manager.
11. (%s1)%s2: access to %s3 failed; stat of '%s4' failed.
12. (%s1)%s2: apr_pollset_poll: (listen)
13. (%s1)%s2: apr_socket_accept: (client socket)
14. (%s1)%s2: ChangeServiceConfig failed
15. (%s1)%s2: Child %s3: Encountered too many errors accepting client connections. Possible causes: %s4. Try using the Win32DisableAcceptEx directive.
16. (%s1)%s2: Child %s3: Failed to acquire the start_mutex. Process will exit.
17. (%s1)%s2: Child %s3: Failure releasing the start mutex
18. (%s1)%s2: could not create %s3
19. (%s1)%s2: could not open mime types config file %s3.
20. (%s1)%s2: could not open transfer log file %s3.
21. (%s1)%s2: Could not resolve host name %s3 -- ignoring!
22. (%s1)%s2: Error starting service control dispatcher
23. (%s1)%s2: Failed to create WinNT Service Profile
24. (%s1)%s2: Failed to open the %s3 Service
25. (%s1)%s2: Failed to open the %s3 Service Manager
26. (%s1)%s2: Failed to resolve server name for %s3 (check DNS) -- or specify an explicit ServerName

27. (%s1)%s2: Failure registering service handler
28. (%s1)%s2: fork: Unable to fork new process
29. (%s1)%s2: GetModuleFileName failed
30. (%s1)%s2: Invalid mime types config path %s3
31. (%s1)%s2: invalid transfer log path %s3.
32. (%s1)%s2: ISAPI: could not create the isapi cache pool
33. (%s1)%s2: make_sock: unable to listen for connections on address %s3
34. (%s1)%s2: master_main: WaitForMultipleObjects with INFINITE wait exited with WAIT_TIMEOUT
35. (%s1)%s2: No installed service named "%s3".
36. (%s1)%s2: OpenService failed
37. (%s1)%s2: Parent: Could not set child process stderr
38. (%s1)%s2: Parent: Could not set child process stdout
39. (%s1)%s2: Parent: ResetEvent(restart_event) failed.
40. (%s1)%s2: Parent: SetEvent for child process %s3 failed.
41. (%s1)%s2: proxy: %s3: attempt to connect to %s4:%s5 (%s6) failed
42. (%s1)%s2: proxy: prefetch request body failed to %s3 (%s4) from %s5 (%s6)
43. (%s1)%s2: Query of Service %s3 failed
44. (%s1)%s2: ResetEvent(shutdown_event)
45. (%s1)%s2: Service %s3 is already started!
46. (%s1)%s2: set_listeners_noninheritable: SetHandleInformation failed.
47. (%s1)%s2: SSL: Failed to generate the certificate monitoring daemon. func=%s3
48. (%s1)%s2: unable to control socket non-blocking status
49. (%s1)%s2: winnt_accept: getsockname error on listening socket, is IPv6 available?
50. [client %s1] (%s2)%s3: access to %s4 denied
51. [client %s1] (%s2)%s3: access to %s4 failed
52. [client %s1] (%s2)%s3: ap_content_length_filter: apr_bucket_read() failed
53. [client %s1] (%s2)%s3: Cannot map %s4 to file
54. [client %s1] (%s2)%s3: copy_brigade_range() failed [%s4-%s5,%s6]
55. [client %s1] (%s2)%s3: core_output_filter: Error reading from bucket.
56. [client %s1] (%s2)%s3: dir_walk error, could not determine the root path of filename %s4%s5 for uri %s6
57. [client %s1] (%s2)%s3: dir_walk error, path_info %s4 is not relative to the filename path %s5 for uri %s6
58. [client %s1] (%s2)%s3: Error reading request entity data
59. [client %s1] (%s2)%s3: file permissions deny server access: %s4
60. [client %s1] (%s2)%s3: proxy: error reading status line from remote server %s4:%s5
61. [client %s1] access to %s2 failed, reason: user '%s3' does not meet 'require'ments for user/valid-user to be allowed access
62. [client %s1] ap_get_server_name: Invalid UCN Option somehow
63. [client %s1] ap_get_server_port: Invalid UCN Option somehow
64. [client %s1] Attempt to serve directory: %s2

65. [client %s1] client sent HTTP/1.1 request without hostname (see RFC2616 section 14.23): %s2
66. [client %s1] client sent invalid HTTP/0.9 request: HEAD %s2
67. [client %s1] Client sent malformed Host header
68. [client %s1] client used wrong authentication scheme: %s2
69. [client %s1] Could not get next bucket brigade [500, #0]
70. [client %s1] Directory index forbidden by Options directive: %s2
71. [client %s1] File does not exist: %s2
72. [client %s1] Forbidden: %s2 doesn't point to a file or directory
73. [client %s1] Invalid method in request %s2
74. [client %s1] Invalid URI in request %s2
75. [client %s1] malformed header from script. Bad header=%s2: %s3
76. [client %s1] meta file permissions deny server access: %s2
77. [client %s1] need AuthName: %s2
78. [client %s1] Negotiation: discovered file(s) matching request: %s2 (None could be negotiated).
79. [client %s1] Premature end of script headers: %s2
80. [client %s1] proxy: %s2 returned by %s3
81. [client %s1] Request exceeded the limit of %s2 internal redirects due to probable configuration error. Use 'LimitInternalRecursion' to increase the limit if necessary. Use 'LogLevel debug' to get a backtrace.
82. [client %s1] Request exceeded the limit of %s2 subrequest nesting levels due to probable configuration error. Use 'LimitInternalRecursion' to increase the limit if necessary. Use 'LogLevel debug' to get a backtrace.
83. [client %s1] request failed: error reading the headers
84. [client %s1] request failed: URI too long (longer than %s2)
85. [client %s1] script not found or unable to stat: %s2
86. [client %s1] Script timed out before returning headers: %s2
87. [client %s1] SSL: Alert message(what?).(%s2,%s3,%s4)
88. [client %s1] SSL: apr_base64_encode error.(%s2,%s3)
89. [client %s1] SSL: apr_base64_encode_len error.(%s2)
90. [client %s1] SSL: Authority error.(%s2,%s3,%s4)
91. [client %s1] SSL: Certificate is invalid.(%s2,%s3,%s4)
92. [client %s1] SSL: Certificate_unknown alert message was received. (%s2,%s3,%s4)
93. [client %s1] SSL: Cipher handshake error.(%s2,%s3,%s4)
94. [client %s1] SSL: Couldn't analyze the client CA certificate.(%s2,%s3,%s4)
95. [client %s1] SSL: Couldn't analyze the client certificate.(%s2,%s3,%s4)
96. [client %s1] SSL: Couldn't get client cert.
97. [client %s1] SSL: Couldn't verify the client CA certificate.(%s2,%s3,%s4)
98. [client %s1] SSL: Couldn't verify the client certificate.(%s2,%s3,%s4)
99. [client %s1] SSL: Error message received(illegal certificate).(%s2,%s3,%s4)
100. [client %s1] SSL: Illegal access protocol.(%s2,%s3,%s4)
101. [client %s1] SSL: MAC verify error.(%s2,%s3,%s4)

102. [client %s1] SSL: No client certificate.(%s2,%s3,%s4)
103. [client %s1] SSL: Not enough memory for base64 encoding.(%s2)
104. [client %s1] SSL: SCMI Insufficient memory
105. [client %s1] SSL: SCMI_Expand failed.(%s2,...%sn)
106. [client %s1] SSL: SCMI_Login failed.(%s2,...%sn)
107. [client %s1] SSL: SCMI_Logout failed.(%s2,...%sn)
108. [client %s1] SSL: Socket access error(%s2).(%s3,%s4,%s5)
109. [client %s1] SSL: The client CA certificate has been revoked.(%s2,%s3,%s4)
110. [client %s1] SSL: The client CA certificate has no path list.(%s2,%s3,%s4)
111. [client %s1] SSL: The client CA certificate path is invalid.(%s2,%s3,%s4)
112. [client %s1] SSL: The client certificate has been revoked.(%s2,%s3,%s4)
113. [client %s1] SSL: The client certificate has expired.(%s2,%s3,%s4)
114. [client %s1] SSL: The client certificate has no path list.(%s2,%s3,%s4)
115. [client %s1] SSL: The client certificate path is invalid.(%s2,%s3,%s4)
116. [client %s1] SSL: Timeout.(%s2,%s3,%s4)
117. [client %s1] SSL: Unacceptable client certificate.(%s2,%s3,%s4)
118. [client %s1] SSL: Unexcepted error.(%s2,%s3,%s4)
119. [client %s1] Symbolic link not allowed or link target not accessible: %s2
120. [client %s1] This resource does not accept the %s2 method.
121. Access to file %s1 denied by server: not a regular file
122. Cannot remove module %s1: not found in module list
123. child process %s1 still did not exit, sending a SIGKILL
124. Configuration Failed
125. could not make child process %s1 exit, attempting to continue anyway
126. Handler for %s1 returned invalid result code %s2
127. Internal error: pcfg_openfile() called with NULL filename
128. Invalid parameters for %s1
129. Must be uid 0 to raise maximum %s1
130. need AuthName: %s1
131. need AuthType to note auth failure: %s1
132. Pre-configuration failed
133. server is within MinSpareThreads of MaxClients, consider raising the MaxClients setting
134. server reached MaxClients setting, consider raising the MaxClients setting
135. SSL: An error has occurred in the SCMI library function.(%s1,%s2,%s3,%s4,%s5,%s6,%s7,%s8,%s9,%s10,%s11,%s12,%s13)
136. SSL: Not enough memory in the SCMI library.
137. SSL: SSL definition acquisition failed.(%s1,SCS_DecryptPassword,%s2)
138. SSL: SSL definition acquisition failed.(%s1,SCS_GetSSLConf,%s2)
139. SSL: SSL definition acquisition failed.(%s1,SCS_GetSSLConf,certconf==NULL)

- 140. [SSL: SSL definition name specification is invalid.\(%s1\)](#)
- 141. [Unable to open logs](#)
- 142. [VirtualHost %s1:%s2 -- mixing * ports and non-* ports with a NameVirtualHost address is not supported, proceeding with undefined results](#)

Explanation and User action of Messages

%s1: could not log pid to file %s2

Variable Information

%s1 = Web server program name

%s2 = Process management file name

Explanation

The process management file (%s2) could not be opened.

System Action

The web server start processing is canceled.

User Action

Refer to the message that was output at the same time and fix the error.

%s1: Service is already installed.

Variable Information

%s1 = Service name

Explanation

The web server service (%s1) has already been registered.

System Action

Web server service registration processing is aborted.

User Action

Check the service (%s1) registration status in the Services window ([Control Panel] > [Administrative Tools] > [Services]).

%s1 not supported on this platform

Variable Information

%s1 = Directive name

Explanation

Directive (%s1) is not supported.

System Action

Web server execution processing is continued.

User Action

Do not use directive (%s1).

(%s1)%s2: %s3: Failed to delete the service.**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service could not be deleted.

System Action

Web server service deletion processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: Failed to open the service.**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service could not be opened.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: Failed to store the ConfigArgs in the registry.**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The registry for the option used when the web server service (%s3) starts could not be registered.

System Action

Web server service registration processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: getrlimit failed

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Directive name

Explanation

The limit for the system resource could not be obtained.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: OpenService failed

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service could not be opened.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: Unable to create the start_mutex.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The exclusive resources for the daemon process could not be created.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: %s3: Unable to start the service manager.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The service control manager failed to start.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: access to %s3 failed; stat of '%s4' failed.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Request URI

%s4 = File name

Explanation

Failed to retrieve the status information for the file (%s4).

System Action

A response is given using status code "403" (Forbidden).

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_pollset_poll: (listen)

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

An error occurred while waiting for the connection from the client.

System Action

The communication process where an error occurred is closed, and web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: apr_socket_accept: (client socket)

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

An attempt to connect to the client socket failed.

System Action

The communication process where an error occurred is closed, and the web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ChangeServiceConfig failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The web server service configuration parameter could not be modified.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Encountered too many errors accepting client connections. Possible causes: %s4. Try using the Win32DisableAcceptEx directive.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID of the daemon process

%s4 = Details information

Explanation

An error occurred in the communication socket wait status transition.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Failed to acquire the start_mutex. Process will exit.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID of the daemon process

Explanation

The exclusive resources for the daemon process could not be acquired.

System Action

The daemon process is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Child %s3: Failure releasing the start mutex

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process ID of the daemon process

Explanation

The exclusive resources for the daemon process could not be released.

System Action

The daemon process is closed.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: could not create %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Process management file name

Explanation

The process management file (%s3) could not be opened.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: could not open mime types config file %s3.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = MIME type settings file name

Explanation

The MIME type settings file (%s3) could not be opened.

System Action

The web server start processing is canceled.

User Action

Check the TypesConfig directive in the environment definition file (httpd.conf). If the TypesConfig directive has been set correctly, resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: could not open transfer log file %s3.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Access log file name

Explanation

The access log file (%s3) could not be opened.

System Action

Web server execution processing is aborted.

User Action

Check the CustomLog directive and the TransferLog directive in the environment definition file (httpd.conf). If the CustomLog directive and the TransferLog directive has been set correctly, resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Could not resolve host name %s3 -- ignoring!

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Host name

Explanation

The name of the virtual host (%s3) could not be resolved.

System Action

Web server execution processing is continued.

User Action

Check if the error details context (%s2) in the host name specified in the <VirtualHost> section or the NameVirtualHost directive of the environment definition file (httpd.conf) is correct.

(%s1)%s2: Error starting service control dispatcher

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to set the service control dispatcher thread.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to create WinNT Service Profile

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The web server service could not be registered.

System Action

Web server service registration processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to open the %s3 Service

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service could not be opened..

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to open the %s3 Service Manager

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = "NT" or "WinNT"

Explanation

A connection could not be established with the service control manager.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to resolve server name for %s3 (check DNS) -- or specify an explicit ServerName

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address

Explanation

The name of IP address (%s3) could not be resolved.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failure registering service handler

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to register the function to process the service control request.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: fork: Unable to fork new process

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The communication process could not be created.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: GetModuleFileName failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The full path of the web server program could not be acquired.

System Action

Web server service registration processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Invalid mime types config path %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = MIME type settings file name

Explanation

The path of the MIME type settings file (%s3) could not be found.

System Action

The web server start processing is canceled.

User Action

Check the TypesConfig directive in the environment definition file (httpd.conf). If the TypesConfig directive has been set correctly, resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: invalid transfer log path %s3.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Access log file name

Explanation

The path of the access log file (%s3) could not be found.

System Action

Web server execution processing is aborted.

User Action

Check the CustomLog directive and the TransferLog directive in the environment definition file (httpd.conf). If the CustomLog directive and the TransferLog directive has been set correctly, resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ISAPI: could not create the isapi cache pool

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The memory management area for the mod_isap module could not be created.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: make_sock: unable to listen for connections on address %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

Explanation

Socket wait status transition failed.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: master_main: WaitForMultipleObjects with INFINITE wait exited with WAIT_TIMEOUT

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

A timeout occurred during daemon process status monitoring.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: No installed service named "%s3".

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name



The error details number (%s1) and the error details context (%s2) "(%s1)%s2: " may not be output.

Explanation

The web server service (%s3) could not be registered.

System Action

Web server execution processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

(%s1)%s2: OpenService failed

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The web server service could not be opened.

System Action

Web server execution processing is aborted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Could not set child process stderr

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to change the configuration for the standard error output of the daemon process.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: Could not set child process stdout

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to change the configuration for the standard output of the daemon process.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: ResetEvent(restart_event) failed.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The event object for restart could not be reset.

System Action

The web server is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Parent: SetEvent for child process %s3 failed.



.....
The period (".") at the end of this message may not be output.
.....

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Daemon process handle

Explanation

The signal status for the event object for stopping the daemon process could not be set.

System Action

The web server is restarted.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: proxy: %s3: attempt to connect to %s4:%s5 (%s6) failed

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Protocol name
%s4 = IP address of remote server
%s5 = Port number of remote server
%s6 = Host name of remote server

Explanation

The remote server connection failed.

System Action

A response is given using status code "502" (Bad Gateway).

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: proxy: prefetch request body failed to %s3 (%s4) from %s5 (%s6)

Variable Information

%s1 = Error details number
%s2 = Error details context
%s3 = Host name of remote server
%s4 = IP address of remote server
%s5 = IP address of systems such as client or proxy server
%s6 = Host name of systems such as client or proxy server



.....
The IP address (%s4) of remote server and the host name (%s6) of systems such as client or proxy server may not be output.
.....

Explanation

The request body from the client or proxy server not be received.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Query of Service %s3 failed

Variable Information

%s1 = Error details number
%s2 = Error details context
%s3 = Service name

Explanation

The web server service (%s3) status could not be obtained.

System Action

The web server stop processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: ResetEvent(shutdown_event)

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The event object for stopping could not be reset.

System Action

The web server is stopped.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Service %s3 is already started!

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

The web server service (%s3) has already been started.

System Action

The web server start processing is canceled.

User Action

This message does not require any action.

(%s1)%s2: set_listeners_noninheritable: SetHandleInformation failed.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The communication socket handle property information could not be set.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: SSL: Failed to generate the certificate monitoring daemon. func=%s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Function name

Explanation

The certificate monitoring daemon could not be generated.

System Action

The web server start processing is canceled.

User Action

Refer to the error details content (%s2), resolve the error, and then restart the web server.

(%s1)%s2: unable to control socket non-blocking status

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to configure the socket as a non-blocking socket.

System Action

The web server start processing is canceled.

User Action

Refer to the error details content (%s2), resolve the error, and then restart the web server.

(%s1)%s2: winnt_accept: getsockname error on listening socket, is IPv6 available?

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

Failed to retrieve the socket information for the IPv6 address.

System Action

Web server execution processing is continued.

User Action

Refer to the error details content (%s2), resolve the error, and then restart the web server.

[client %s1] (%s2)%s3: access to %s4 denied**Variable Information**

- %s1 = IP address of systems such as client or proxy server
- %s2 = Error details number
- %s3 = Error details context
- %s4 = Request URI

Explanation

Access to the directory that was used to store the contents is not allowed.

System Action

A response is given using status code "403" (Forbidden).

User Action

To allow access, check the directory access authority.

[client %s1] (%s2)%s3: access to %s4 failed**Variable Information**

- %s1 = IP address of systems such as client or proxy server
- %s2 = Error details number
- %s3 = Error details context
- %s4 = Request URI

Explanation

The directory or file in which the contents have been stored could not be accessed.

System Action

A response is given using status code "403" (Forbidden).

User Action

Check the error details context (%s3) that are output, and take the action described in the following table.

Error Details Context (%s3)	Meaning / Required Action
Value too large for defined data type	A file bigger than 2GB was accessed - such files cannot be used as content. Ensure that the files are smaller than 2GB.
All other cases	Resolve the cause of the error according to the error details context (%s3).

[client %s1] (%s2)%s3: ap_content_length_filter: apr_bucket_read() failed

Or

[client %s1] (%s2)%s3: ap_content_length_filter: apr_bucket_read() failed, referer: %s4 **Note**

.....
If the referer header was received from the client or proxy server, ", referer: %s4" is added after the message body, and the referer header value (%s4) is also output.
.....

Variable Information

- %s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = referrer header value

Explanation

The data during output filter processing could not be read.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

Check the error details context (%s3) that are output, and take the action described in the following table.

Error Details number (%s2)	Error Details Context (%s3)	Meaning / Required Action
Linux32/64 104	Linux32/64 Connection reset by peer	Refer to the access log or the trace log, and check if a request to the CGI program has been received when this error occurs. If a request to the CGI program was received, processing may have ended without the CGI program reading the request message body. If this problem occurs, the display of the CGI program execution results in the client may also be delayed. Take the following action: To suppress the output of this error and the delay in the display of the CGI program execution results, correct the CGI program so that it reads the request message body. To only suppress the delay in the display of the CGI program execution results, disable the HTTP Keep-Alive feature (*1) and then restart the web server. If a request to the CGI program was not received, collect the diagnostic information using the <i>iscollectinfo</i> command, and contact your SE (systems engineer) .
All other cases		Resolve the cause of the error according to the error details context (%s3).

*1: If the KeepAlive directive setting in the environment definition file (httpd.conf) is "On", change it to "Off".

[client %s1] (%s2)%s3: Cannot map %s4 to file

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = Request line

Explanation

Failed to retrieve the absolute path of the contents file from the request URI.

System Action

A response is given using status code "403" (Forbidden).

User Action

Check the DocumentRoot directive in the environment definition file (httpd.conf).

[client %s1] (%s2)%s3: copy_brigade_range() failed [%s4-%s5,%s6]**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = Specified range starting point

%s5 = Specified range ending point

%s6 = Context size

Explanation

Failed to create the response data from starting point %s4 to ending point %s5 that are specified in the Range or Request-Range header field.

System Action

One of the following processing types will be performed:

- If the processing for all the specified ranges that are specified in the request fails, a reply using status code "416" (Requested Range Not Satisfiable) is returned.
- If the processing for some of the specified ranges that are specified in the request fails, a reply using status code "206" (Partial Content), and the response data for the specified range content for which processing succeeded is returned.

User Action

Resolve the cause of the error according to the error details context (%s3).

[client %s1] (%s2)%s3: core_output_filter: Error reading from bucket.**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

Explanation

The data during output filter processing could not be read.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Resolve the cause of the error according to the error details context (%s2).

[client %s1] (%s2)%s3: dir_walk error, could not determine the root path of filename %s4%s5 for uri %s6**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = File path information 1

%s5 = File path information 2

%s6 = Request URI

Explanation

An error occurred in directory section processing.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Resolve the cause of the error according to the error details context (%s2).

[client %s1] (%s2)%s3: dir_walk error, path_info %s4 is not relative to the filename path %s5 for uri %s6

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

%s4 = File path information 1

%s5 = File path information 2

%s6 = Request URI

Explanation

An error occurred during directory section processing.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Resolve the cause of the error according to the error details context (%s2).

[client %s1] (%s2)%s3: Error reading request entity data

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Error details number

%s3 = Error details context

Explanation

The request body could not be read.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take the following actions:

- Request that the user of the client (%s1) specify a correct request body.

- A timeout may have occurred while the request body was being received. Check the value set for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] (%s2)%s3: file permissions deny server access: %s4

Variable Information

- %s1 = IP address of systems such as client or proxy server
- %s2 = Error details number
- %s3 = Error details context
- %s4 = File name of the requested content

Explanation

Access to the requested contents (%s4) is not allowed.

System Action

A response is given using status code "403" (Forbidden).

User Action

To allow access, check the file authority.

[client %s1] (%s2)%s3: proxy: error reading status line from remote server %s4:%s5

Or

[client %s1] (%s2)%s3: proxy: error reading status line from remote server %s4:%s5, referer: %s6



.....
If the referer header was received from the client or proxy server, ", referer: %s6" is added after the message body, and the referer header value (%s6) is also output.
.....

Variable Information

- %s1 = IP address of systems such as client or proxy server
- %s2 = Error details number
- %s3 = Error details context
- %s4 = Host name or IP address of remote server
- %s5 = Port number of remote server
- %s6 = referrer header value

Explanation

Failed to read the status line in the response from the remote server.

System Action

A response is given using status code "502" (Bad Gateway).

User Action

Check the following values:

- The value set for the Timeout directive in the environment definition file (httpd.conf).
- The output results for the item "Duration from acceptance of a request to completion of processing", which is output to the access log at the time of the response from the remote server.

If the above values match, a timeout may have occurred during the wait for the response from the remote server. Check whether an error has occurred in the network or remote server.

If the above values do not match, check whether there is a problem in the response from the remote server.

[client %s1] access to %s2 failed, reason: user '%s3' does not meet 'require'ments for user/valid-user to be allowed access

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = URI name

%s3 = User name

Explanation

The user (%s3) that made the request for the URI (%s2) is not allowed access.

System Action

A response is given using status code "401" (Authorization Required).

User Action

Take the following actions:

- If "user userid" is specified for the Require directive in the environment definition file (httpd.conf), ensure that the user (%s3) was set for userid.
- If "group group-name" is specified for the Require directive in the environment definition file (httpd.conf), make sure that it is also set in the file specified in the AuthGroupFile directive and that the user (%s3) was set in the group. If the group/user (%s3) was not set in the file, set it to provide access.

[client %s1] ap_get_server_name: Invalid UCN Option somehow

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The value set for the UseCanonicalName directive in the environment definition file (httpd.conf) is incorrect. The ServerName directive requires a value of "localhost".

System Action

Web server execution processing is continued.

User Action

Check the value set for the UseCanonicalName directive in the environment definition file (httpd.conf).

[client %s1] ap_get_server_port: Invalid UCN Option somehow

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The value set for the UseCanonicalPhysicalPort directive in the environment definition file (httpd.conf) is incorrect. The default port number is used as the port number that is defined for the ServerName directive.

System Action

Web server execution processing is continued.

User Action

Check the value set for the UseCanonicalPhysicalPort directive in the environment definition file (httpd.conf).

[client %s1] Attempt to serve directory: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Requested content

Explanation

The requested content (%s2) is a directory.

System Action

A response is given using status code "404" (Not Found).

User Action

Request that the user of the client specifies a correct URI.

[client %s1] client sent HTTP/1.1 request without hostname (see RFC2616 section 14.23): %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request URI

Explanation

The Host header that is essential for HTTP/1.1 has not been specified.

System Action

A response is given using status code "400" (Bad Request).

User Action

Request that the user of the client specifies a correct Host header.

[client %s1] client sent invalid HTTP/0.9 request: HEAD %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request URI

Explanation

The required HTTP version has not been specified for the HEAD method.

System Action

A response is given using status code "400" (Bad Request).

User Action

Request that the user of the client specifies the HTTP version on the request line.

[client %s1] Client sent malformed Host header

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The specified Host header is incorrect.

System Action

A response is given using status code "400" (Bad Request).

User Action

Request that the user of the client specifies the Host header using the correct format.

[client %s1] client used wrong authentication scheme: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request URI

Explanation

An incorrect authentication type was specified in the request header.

System Action

A response is given using status code "401" (Authorization Required).

User Action

Request that the user of the client specifies the correct authentication type.

[client %s1] Could not get next bucket brigade [500, #0]

Variable Information

%s1 = IP address of system such as client or proxy server

Explanation

Failed to read the request body of the WebDAV request.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take the following actions:

- Request that the user of the client (%s1) specify a correct request body.
- A timeout may have occurred while the request body was being received. Check the value set for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] Directory index forbidden by Options directive: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Requested path name

Explanation

A forward slash (/) was specified at the end of the URI, however in this case the file set as the search target (the value set for the DirectoryIndex directive) did not exist. Additionally, the setting for the automatic generation of the directory list (the list of directory content) was disabled.



Even if the forward slash (/) has not been specified at the end of the URI, it still might have been added automatically.

System Action

A response is given using status code "403" (Forbidden).

User Action

Take the following actions:

- Instruct the user to add the file name to the request to the specified client.
- If the forward slash (/) was specified at the end of the requested URI and there is a response from the search target file, place the file specified in the environment definition file (httpd.conf) DirectoryIndex directive in %s2.
- To display the directory list, specify the Indexes (or All) option in the environment definition file (httpd.conf) Options directive so that the setting for the automatic generation of the directory list will be enabled.

[client %s1] File does not exist: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Requested content

Explanation

The requested content (%s2) does not exist.

System Action

A response is given using status code "404" (Not Found).

User Action

Check the requested content (%s2) that are output, and take the action described in the following table.

Requested Content (%s2)	Meaning / Required Action
favicon.ico	An icon required on the web browser (Favorites, Address Bar, Tab) does not exist. To display the icon on the web browser, place the "favicon.ico" icon in the directory specified in the environment definition file (httpd.conf) DocumentRoot directive. No action is necessary if the icon does not need to be displayed.
All other cases	The URI specified in the client may be incorrect. Request that the user of the client specifies the correct URI. A URI that does not exist may have been accessed because of the search engine information collection program (crawler), a client feature (such as the browser), or

Requested Content (%s2)	Meaning / Required Action
	a program used to launch attacks, even if the URI specified in the client is correct. Check that there are no problems in the URI and client (%s1) environment.

[client %s1] Forbidden: %s2 doesn't point to a file or directory

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Requested content

Explanation

The requested content (%s2) is not a file or directory.

System Action

A response is given using status code "403" (Forbidden).

User Action

Check the content storage directory.

[client %s1] Invalid method in request %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request line

Explanation

The specified request method is incorrect.

System Action

A response is given using status code "501" (Method Not Implemented).

User Action

Request that the user of the client specifies the correct method.

[client %s1] Invalid URI in request %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request line

Explanation

The specified URI is incorrect.

System Action

A response is given using status code "400" (Bad Request).

User Action

Request that the user of the client specifies a correct URI.

[client %s1] malformed header from script. Bad header=%s2: %s3

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Header in the response from CGI

%s3 = CGI program path name

Explanation

There is no colon (:) in the response header (%s2) that was returned from the CGI program (%s3).

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Check that the response header (%s2) that was returned from the CGI program (%s3) is correct.

[client %s1] meta file permissions deny server access: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = File name of requested content

Explanation

Access to the requested contents (%s2) is not allowed.

System Action

A response is given using status code "403" (Forbidden).

User Action

To allow access, check the file authority.

[client %s1] need AuthName: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request URI

Explanation

The AuthName directive in the environment definition file (httpd.conf) must be specified.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Set the AuthName directive in the environment definition file (httpd.conf).

[client %s1] Negotiation: discovered file(s) matching request: %s2 (None could be negotiated).

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request content

Explanation

The request content (%s2) does not exist. An invalid URI may have been specified in the client.

System Action

A response is given using status code "403" (Not Found).

User Action

Check if an incorrect URI has been specified for the client %s1. If the URI is incorrect, specify the correct URI.

[client %s1] Premature end of script headers: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = CGI program name

Explanation

Not all of the header information output by the CGI program could be received.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take one of the following actions:

- Check the CGI program.
- A timeout may have occurred while the CGI program was running. Check the value set for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] proxy: %s2 returned by %s3

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Detail information

%s3 = Request URI

Explanation

One of the following causes is assumed:

Detail information (%s2)	Causes
user credentials contained invalid character	The user name/password for the request (%s3) contains invalid characters.
All other cases	an error has occurred in the request (%s3).

System Action

A response is made with the following status codes:

Detail information (%s2)	Status Codes
user credentials contained invalid character	"400" (Proxy Error)

Detail information (%s2)	Status Codes
All other cases	"400"/"401"/"403"/"404"/"501"/"502"/"503" (Proxy Error)

User Action

Take one of the following actions:

Detail information (%s2)	User Action
user credentials contained invalid character	Instruct the user to specify the correct user name/password for %s1.
All other cases	Resolve the cause of the error according to %s2.

[client %s1] Request exceeded the limit of %s2 internal redirects due to probable configuration error. Use 'LimitInternalRecursion' to increase the limit if necessary. Use 'LogLevel debug' to get a backtrace.

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Limit for the number of internal directories

Explanation

The number of internal directories has exceeded limit (%s2).

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take the following actions:

- Check the definition to ensure that the number of internal redirects does not exceed the limit.
- An illegal request may have been received. In the IP access control settings, set the IP address of the client recorded in the error log to deny access.

[client %s1] Request exceeded the limit of %s2 subrequest nesting levels due to probable configuration error. Use 'LimitInternalRecursion' to increase the limit if necessary. Use 'LogLevel debug' to get a backtrace.

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Limit for the number of subrequests

Explanation

The number of subrequests has exceeded limit (%s2).

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take the following actions:

- Check the definition to ensure that the number of subrequests does not exceed the limit.

- An illegal request may have been received. In the IP access control settings, set the IP address of the client recorded in the error log to deny access.

[client %s1] request failed: error reading the headers

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The request header could not be read.

System Action

A response is given using status code "400" (Bad Request).

User Action

Take one of the following actions:

- Request that the user of the client specifies the correct request header.
- A timeout may have occurred while the request header was being received. Check the value set for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] request failed: URI too long (longer than %s2)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Maximum size of the request line

Explanation

The length of the request line has exceeded the maximum size (%s2).

System Action

A response is given using status code "414" (Request-URI Too Large).

User Action

Take one of the following actions:

- Request that the user of the client specifies a request line that does not exceed the maximum size.
- Check the value set for the LimitRequestLine directive in the environment definition file (httpd.conf).

[client %s1] script not found or unable to stat: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request CGI program

Explanation

%s2 does not exist - an invalid URI might have been specified in %s1.

System Action

A response is given using status code "404" (Not Found).

User Action

Request that the user of the client (%s1) specify a correct URI.

[client %s1] Script timed out before returning headers: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = CGI program name

Explanation

A timeout may have occurred while the CGI program was running.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Take one of the following actions:

- Check the CGI program.
- Check the value set for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] SSL: Alert message(what?).(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

An Alert message was received from client (%s1) because an error occurred in the client (%s1).

System Action

Communication is closed.

User Action

Check whether the status of the client (%s1) is an error status.

[client %s1] SSL: apr_base64_encode error.(%s2,%s3)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Detail information 1

%s3 = Detail information 2

Explanation

The client certificate could not be launched. The data received from the client (%s1) may be corrupt.

System Action

Communication is closed.

User Action

Check whether there is a problem in the network or client.

[client %s1] SSL: apr_base64_encode_len error.(%s2)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Detail information

Explanation

The client certificate could not be launched. The data received from the client (%s1) may be corrupt.

System Action

Communication is closed.

User Action

Check whether there is a problem in the network or client.

[client %s1] SSL: Authority error.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Due to one of the following reasons, an authentication error occurred when the web server tried to reference the client CA certificate on the server.

1. Environment setting of SSL (creation of a certificate and key control environment, creation of a private key and acquisition of a certificate, registration of a certificate and CRL) was executed with administrator authority.
2. The user who set up the SSL environment (other than administrator authority) is not specified in the User/Group directive in the environment setting file (httpd.conf) of the web server.

System Action

Communication is closed.

User Action

Take one of the following actions:

1. Environment setting of SSL (creation of a certificate and key control environment, creation of a private key and acquisition of a certificate, and registration of a certificate and CRL) should be performed by a user other than one with administrator authority.

If an Interstage certificate environment is used, specify the -g option and ensure that the Interstage certificate environment owner group has been set when the Interstage certificate environment is built using the *scsmakeenv* command. For details on the Interstage certificate environment privileges settings, refer to the Security System Guide.

After that, take the action shown in Item 2.

- Specify the user who setup the SSL environment (other than administrator authority) in the User/Group directive in the environment setting file (httpd.conf).

[client %s1] SSL: Certificate is invalid.(%s2,%s3,%s4)**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

A problem occurred in the client (%s1) and the client (%s1) then sent an Alert message.

System Action

Communication is closed.

User Action

Check whether the client (%s1) has a normal status.

[client %s1] SSL: Certificate_unknown alert message was received. (%s2,%s3,%s4)**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The certificate_unknown Alert message was received from the client (%s1).

System Action

Communication is closed.

User Action

An error, such as failure to validate the site certificate, may have occurred in the client (%s1), therefore communication from the client (%s1) was disconnected.

Check that the web server CA certificate was registered correctly in the client (%s1).

If the web server CA certificate was registered correctly in the client (%s1), investigate the cause of the sending of the certificate_unknown Alert message to the client (%s1).

[client %s1] SSL: Cipher handshake error.(%s2,%s3,%s4)**Variable Information**

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The connection was not received because the encryption method for the request sent from the client (%s4) is not allowed in the web server.

System Action

Communication is closed.

User Action

Take one of the following actions:

- Check whether the encryption method set in the web server can be used in the client (%s4).
- Perform the following steps to check whether the encryption method for allowing the connection has been set correctly.

For the Interstage certificate environment:

1. In the Interstage Management Console, click [Security] > [SSL] > [SSL definition].
2. Click the [SSL Detailed Settings] button on the displayed [SSL definition: SSL Configuration Settings] page, and check the [Encryption Method].

For a certificate/key management environment configured with the SMEE command:

1. Check the SSLCipherSuite directive that is set in the environment definition file (httpd.conf).

[client %s1] SSL: Couldn't analyze the client CA certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Analysis of the client CA certificate failed.

System Action

Communication is closed.

User Action

Obtain a new CA certificate from the CA, and reregister the newly obtained CA certificate

[client %s1] SSL: Couldn't analyze the client certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Analysis of the client certificate failed. The client certificate sent from the client may have been damaged.

System Action

Communication is closed.

User Action

Connection to the client on which this client certificate is registered cannot be established.

To connect to this client, request that the CA issue a client certificate, and register the obtained certificate on this client.

[client %s1] SSL: Couldn't get client cert.

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The client certificate could not be obtained.

System Action

Communication is closed.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

[client %s1] SSL: Couldn't verify the client CA certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Verification of the client CA certificate failed.

System Action

Communication is closed.

User Action

Verify that the client CA certificate relationship for this route is correct.

[client %s1] SSL: Couldn't verify the client certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Detection of the client certificate and client CA certificate registered on the client and in the key management environment failed.

System Action

Communication is closed.

User Action

Verify that the relationship between the client certificate and the client CA certificate is correct.

If the client CA certificate is incorrect, obtain a new CA certificate from the CA, and reregister the newly obtained CA certificate.

If the client certificate is incorrect, request that the CA issue the client certificate, and reregister the obtained client certificate

[client %s1] SSL: Error message received(illegal certificate).(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

A problem occurred in the client (%s1) and the client (%s1) sent an Alert message.

System Action

Communication is closed.

User Action

Check whether the client (%s1) has a normal status.

[client %s1] SSL: Illegal access protocol.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The SSL port was accessed using a protocol that is not SSL.

System Action

Communication is closed.

User Action

Check whether there is a problem with the specified protocol in client (%s1).

[client %s1] SSL: MAC verify error.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Failed to verify the client data. The data received from the client (%s1) may be corrupt.

System Action

Communication is closed.

User Action

Check whether there is an error in the network or client.

[client %s1] SSL: No client certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The client certificate cannot be received from the client (%s1) because either:

- The client certificate is not registered on the client (%s1).
- The client operator refused to send the client certificate.

System Action

Communication is closed.

User Action

Take one of the following actions:

- To connect to this client (%s1), request that the CA issue a client certificate, and register the obtained certificate on this client.
- If the client operator refused to send the client certificate, no action is required.

[client %s1] SSL: Not enough memory for base64 encoding.(%s2)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Detail information

Explanation

The client certificate could not be launched.

System Action

Communication is closed.

User Action

Check that there is sufficient memory. If there is insufficient memory, close unnecessary programs and secure the required memory capacity for running the web server.

[client %s1] SSL: SCMI Insufficient memory

Variable Information

%s1 = IP address of systems such as client or proxy server

Explanation

The client certificate could not be launched.

System Action

Communication is closed.

User Action

Check that there is sufficient memory. If there is insufficient memory, close unnecessary programs and secure the required memory capacity for running the web server.

[client %s1] SSL: SCMI_Expand failed.(%s2,...%sn)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 - %sn = Extra information

Explanation

An error occurred while calling the SCMI function. An error may have occurred for the certificate and key control environment.

System Action

Communication is closed.

User Action

Check the certificate and key control environment.

If this error message continues to be displayed, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

[client %s1] SSL: SCMI_Login failed.(%s2,...%sn)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 - %sn = Extra information

Explanation

An error occurred while calling the SCMI function. An error may have occurred for the certificate and key control environment.

System Action

Communication is closed.

User Action

Check the certificate and key control environment.

If this error message continues to be displayed, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

[client %s1] SSL: SCMI_Logout failed.(%s2,...%sn)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 - %sn = Extra information

Explanation

An error occurred while calling the SCMI function. An error may have occurred for the certificate and key control environment.

System Action

Communication is closed.

User Action

Check the certificate and key control environment.

If this error message continues to be displayed, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

[client %s1] SSL: Socket access error(%s2).(%s3,%s4,%s5)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Socket function name

%s3 = SSL function name

%s4 = Error code

%s5 = Detail code

Explanation




An error occurred accessing the socket during the SSL application.

System Action

Communication is closed.

User Action

Check the SSL function (%s3), the error code (%s4), and the detail code (%s5) that are output, and take the action described in the following table.

SSL function (%s3)	Error code (%s4)	Detail code (%s5)	Meaning / Required Action
SSL_ServerHandshake	 Windows32/64 00400006	00002745	The connection to the client (%s1) may have been lost. Check the status of the connection to the client (%s1).
	 Solaris32/64 00400006	00000020	
	 Solaris32/64 00400007	00000083	
All other cases			Collect diagnostic information using the <i>iscollectinfo</i> command, and contact your SE (systems engineer) .

[client %s1] SSL: The client CA certificate has been revoked.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The client CA certificate is revoked.

System Action

Communication is closed.

User Action

Obtain a new CA certificate from the CA, and reregister the newly obtained CA certificate.

[client %s1] SSL: The client CA certificate has no path list.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The certificate pathway for the client CA certificate does not exist.

System Action

Communication is closed.

User Action

Register the client CA certificate in the certificate/key management environment starting with the root CA.

[client %s1] SSL: The client CA certificate path is invalid.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The certificate pathway for the client CA certificate is incomplete.

System Action

Communication is closed.

User Action

Register the client CA certificate in the certificate/key management environment starting with the root CA.

[client %s1] SSL: The client certificate has been revoked.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Client access was rejected because a client certificate that had been invalidated by the CA was received.

System Action

Communication is closed.

User Action

Connection cannot be established with the client to which this client certificate is registered. To connect to this client, request that the CA issue a client certificate, and register the obtained certificate on the client.

[client %s1] SSL: The client certificate has expired.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Client (%s1) access was rejected because an expired client certificate was received.

System Action

Communication is closed.

User Action

Connection cannot be established with the client to which this client certificate is registered. To connect to this client, request that the CA issue a client certificate, and register the obtained certificate on this client (%s1).

[client %s1] SSL: The client certificate has no path list.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The certificate pathway for the client certificate does not exist.

System Action

Communication is closed.

User Action

Register the client CA certificate in the certificates and key management environment sequentially from the root CA.

[client %s1] SSL: The client certificate path is invalid.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

The certificate pathway for the client certificate is incomplete.

System Action

Communication is closed.

User Action

Register the client CA certificate in the certificates and key management environment sequentially from the root CA.

[client %s1] SSL: Timeout.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

A timeout occurred in SSL communication.

System Action

Communication is closed.

User Action

Check the client status.

If this message is output frequently, increase the value for the Timeout directive in the environment definition file (httpd.conf).

[client %s1] SSL: Unacceptable client certificate.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

Client access was rejected because the CA certificate of the client certificate sent from the client was not registered in the certificates and key management environment.

System Action

Communication is closed.

User Action

Register the CA certificate of the client certificate in the certificates and key management environment using the certificate and CRL management command.

[client %s1] SSL: Unexcepted error.(%s2,%s3,%s4)

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Function name

%s3 = Error code

%s4 = Detail code

Explanation

An unexpected error occurred in the SSL function.

System Action

Communication is closed.

User Action

Check the function name (%s2) and error code (%s3) that are output, and take the action described in the following table.

Function Name (%s2)	Error Code (%s3)	Meaning / Required Action
SSL_ServerHandshake	0030001D	The client certificate, or signature information of the client certificate, sent from the client (%s1) is invalid. Check whether there is a problem with the client certificate used in the client (%s1).
	00500002	Invalid data was received from the client (%s1).
	00500009	Check if there is a problem with the data sent from the client (%s1).
	0050000B	
	0050000C	
	0050001C	
	0050000D	Access from the client (%s1) may have used a protocol other than "https". Check if there is a problem with the protocol used.
00700001	An error occurred in the client (%s1), therefore the Alert message was received from the client (%s1). Check whether the client (%s1) has error status.	
00700002	Illegal data was received from the client (%s1), therefore the Alert message was sent to the client (%s1). Check whether there is a problem with the data that was sent from the client (%s1).	
00800002	The connection may have been closed by the client (%s1).	

Function Name (%s2)	Error Code (%s3)	Meaning / Required Action
		Check the state of the connection with the client (%s1).
SSL_Read or SSL_Write	00700001	An error occurred in the client (%s1), therefore the Alert message was received from the client (%s1). Check whether there is a problem with the data that was sent from the client (%s1).
	00700002	Illegal data was received from the client (%s1), therefore the Alert message was sent to the client (%s1). Check whether there is a problem with the data that was sent from the client (%s1).
	00800002	The connection may have been closed by the client (%s1). Check the state of the connection with the client (%s1).
All other cases		Collect diagnostic information using the <i>iscollectinfo</i> command, and contact your SE (systems engineer) .

[client %s1] Symbolic link not allowed or link target not accessible: %s2

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Symbolic link path

Explanation

Access to symbolic link (%s2) is not allowed.

System Action

A response is given using status code "403" (Forbidden).

User Action

If the link destination for the symbolic link does not exist, deploy a link destination.

To allow access to the symbolic link, set FollowSymLinks in the Options directive of the environment definition file (httpd.conf).

[client %s1] This resource does not accept the %s2 method.

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Request method

Explanation

The request method (%s2) is not allowed.

System Action

A response is given using status code "405" (Method Not Allowed).

User Action

Ask the user of the client to specify a method that is allowed.

Access to file %s1 denied by server: not a regular file

Variable Information

%s1 = File name

Explanation

Access to the file (%s1) is not allowed.

User Action

To allow access, check the file access authority.

Cannot remove module %s1: not found in module list

Variable Information

%s1 = Plug-in module name

Explanation

The plug-in module (%s1) cannot be deleted because it is not in the module list.

System Action

The web server start or stop processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

child process %s1 still did not exit, sending a SIGKILL

Variable Information

%s1 = Process ID of the communication process

Explanation

The communication process does not close.

System Action

This message does not require any action.

User Action

Not required.

Configuration Failed

Explanation

An error occurred in initialization processing.

System Action

Web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

could not make child process %s1 exit, attempting to continue anyway

Variable Information

%s1 = Process ID of the communication process

Explanation

The expected communication process close is not performed.

System Action

Communication process close processing is aborted.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

Handler for %s1 returned invalid result code %s2

Variable Information

%s1 = Handler name

%s2 = Value returned by the handler

Explanation

The handler (%s1) returned a function as the return value (%s2).

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Third-party plug-in modules, including mod_perl and mod_php, are not supported. Only the plug-in modules provided in the Fujitsu product can be used.

If the installed plug-in module is not supported, none of the web server operations will be supported either.

Internal error: pcfgr_openfile() called with NULL filename

Explanation

An internal error occurred in file open processing.

User Action

Refer to the message that was output at the same time and fix the error.

Invalid parameters for %s1

Variable Information

%s1 = Directive name

Explanation

The directive (%s1) parameter is incorrect.

System Action

Web server execution processing is continued.

User Action

Check the parameter of directive (%s1).

Must be uid 0 to raise maximum %s1

Variable Information

%s1 = Directive name

Explanation

Failed to configure a value for the system resource upper limit (hardware limit).

System Action

Web server execution processing is continued.

User Action

A value that exceeds the system resource upper limit (hardware limit) cannot be configured.

need AuthName: %s1

Variable Information

%s1 = Request URI

Explanation

The AuthName directive in the environment definition file (httpd.conf) must be specified.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Set the AuthName directive in the environment definition file (httpd.conf).

need AuthType to note auth failure: %s1

Variable Information

%s1 = Request URI

Explanation

The AuthType directive in the environment definition file (httpd.conf) must be specified.

System Action

A response is given using status code "401" (Authorization Required).

User Action

Set the AuthType directive in the environment definition file (httpd.conf).

Pre-configuration failed

Explanation

An error occurred in initialization preprocessing.

System Action

Web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

server is within MinSpareThreads of MaxClients, consider raising the MaxClients setting

Explanation

The number of communication processes has reached the upper limit.

Note

.....

This message is output the first time the number of requests reaches the upper limit for the number of simultaneous connections after the web server starts up. Once this message is output, it is not output again until the web server restarts.

.....

System Action

Web server execution processing is continued.

User Action

- Check the value set for the following directive in the environment definition file (httpd.conf) if necessary.
- MaxClients
- ThreadsPerChild

Point

.....

The value configured as the upper limit for the number of communication processes is calculated using the following formula:

$\text{Upper limit for the number of communication processes} = \frac{\text{Value set in the MaxClients directive}}{\text{Value set in the ThreadsPerChild directive}}$

(Digits after the decimal point: Truncated)

.....

server reached MaxClients setting, consider raising the MaxClients setting

Explanation

The number of communication processes has reached the number of simultaneous connections limit set for the MaxClients directive in the environment definition file (httpd.conf).

Note

.....

This message is output the first time the number of requests reaches the upper limit for the number of simultaneous connections after the web server starts up. Once this message is output, it is not output again until the web server restarts.

.....

System Action

Web server execution processing is continued.

User Action

Check the value set for the MaxClients directive if necessary.

SSL: An error has occurred in the SCMI library function. (%s1,%s2,%s3,%s4,%s5,%s6,%s7,%s8,%s9,%s10,%s11,%s12,%s13)

Variable Information

%s1 = SCMI library function name

%s2 -%s13 =Additional information

Explanation

An error occurred in the SCMI library function (%s1). The certificate/key management environment may be invalid.

System Action

The web server start processing is canceled.

User Action

Check whether the certificate/key management environment settings are valid. If the certificate/key management environment settings are valid, collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

SSL: Not enough memory in the SCMI library.

Explanation

The SCMI library memory became insufficient.

System Action

The web server start processing is canceled.

User Action

Check that there is sufficient memory. If there is insufficient memory, close unnecessary programs and secure the required memory capacity for running the web server.

SSL: SSL definition acquisition failed.(%s1,SCS_DecryptPassword,%s2)

Variable Information

%s1 = SSL definition name

%s2 = Error details context

Explanation

SSL definition (%s1) certificate information failed to be acquired.

System Action

The web server start processing is canceled.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

SSL: SSL definition acquisition failed.(%s1,SCS_GetSSLConf,%s2)

Variable Information

%s1 = SSL definition name

%s2 = Error details context

Explanation

SSL definition (%s1) certificate information failed to be acquired.

System Action

The web server start processing is canceled.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

SSL: SSL definition acquisition failed.(%s1,SCS_GetSSLConf,certconf==NULL)

Variable Information

%s1 = SSL definition name

Explanation

SSL definition (%s1) certificate information failed to be acquired.

System Action

The web server start processing is canceled.

User Action

Collect diagnostic information using the *iscollectinfo* command, and then contact your systems engineer.

SSL: SSL definition name specification is invalid.(%s1)

Variable Information

%s1 = SSL definition name

Explanation

The SSL definition (%s1) does not exist.

System Action

The web server start processing is canceled.

User Action

Check whether the Interstage certificate environment has been set up correctly.

If it has, specify the correct SSL definition name for the SSLConfName directive in the environment definition file (%s2).

Unable to open logs

Explanation

An error occurred in log initialization processing. The File Descriptor number required to run the web server may be invalid.

System Action

Web server execution processing is aborted.

User Action

Refer to the message that was output at the same time and fix the error.

VirtualHost %s1:%s2 -- mixing * ports and non-* ports with a NameVirtualHost address is not supported, proceeding with undefined results

Variable Information

%s1 = Virtual host name

%s2 = Port number

Explanation

Asterisks (*) and non-asterisks cannot be specified together in the namebase virtual host port number settings.

System Action

Web server execution processing is continued.

User Action

Check the port number specified for the <VirtualHost> section and the NameVirtualHost directive in the environment definition file (httpd.conf).

8.10.5 Messages Whose Log Levels are "warn"

The meaning and user action for log level "warn" is explained.

Message list

1. %s1: apr_gethostname() failed to determine ServerName
2. %s1: apr_sockaddr_info_get() failed for %s2
3. (%s1)%s2: connect to listener on %s3
4. (%s1)%s2: disk_cache: rename tempfile to datafile failed: %s3 -> %s4
5. (%s1)%s2: Failed to enable APR_TCP_DEFER_ACCEPT
6. (%s1)%s2: Failed to enable the '%s3' Accept Filter
7. (%s1)%s2: make_sock: failed to set ReceiveBufferSize for address %s3, using default
8. (%s1)%s2: make_sock: failed to set SendBufferSize for address %s3, using default
9. (%s1)%s2: mpm_get_completion_context: CreateEvent failed.
10. (%s1)%s2: mpm_get_completion_context: Failed to create the transaction pool.
11. (%s1)%s2: No installed ConfigArgs for the service "%s3", using Apache defaults.
12. (%s1)%s2: setsockopt(SO_UPDATE_ACCEPT_CONTEXT) failed.
13. (%s1)%s2: sigaction(%s3)
14. (%s1)%s2: winnt_accept: Asynchronous AcceptEx failed.
15. (%s1)%s2: winnt_accept: Failed to allocate an accept socket. Temporary resource constraint? Try again.
16. (%s1)%s2: write pipe_of_death
17. [client %s1] handler "%s2" not found for: %s3
18. _default_VirtualHost overlap on port %s1, the first has precedence
19. child process %s1 still did not exit, sending a SIGTERM
20. integer overflow or out of memory condition.
21. Limiting internal redirects to very low numbers may cause normal requests to fail.
22. Limiting the subrequest depth to a very low level may cause normal requests to fail.
23. long lost child came home! (pid %s1)
24. NameVirtualHost %s1:%s2 has no VirtualHosts
25. pid file %s1 overwritten -- Unclean shutdown of previous Apache run?
26. Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting
27. SSL: The CA certificate validity term has expired.(%s1,%s2/%s3/%s4 %s5:%s6:%s7)
28. SSL: The CA certificate will expire in %s1 days.(%s2,%s3/%s4/%s5 %s6:%s7:%s8)
29. SSL: The site certificate validity term has expired.(%s1,%s2/%s3/%s4 %s5:%s6:%s7)

30. **SSL:** The site certificate will expire in %s1 days.(%s2,%s3/%s4/%s5 %s6:%s7:%s8)
31. **VirtualHost %s1:%s2 overlaps with VirtualHost %s3:%s4, the first has precedence, perhaps you need a NameVirtualHost directive**
32. **WARNING:** Attempt to change ServerLimit or ThreadLimit ignored during restart
33. **WARNING:** Attempt to change ThreadLimit ignored during restart

Explanation and User action of Messages

%s1: apr_gethostname() failed to determine ServerName

Variable Information

%s1 = Name of web server execution program

Explanation

The local host name could not be obtained.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

%s1: apr_sockaddr_info_get() failed for %s2

Variable Information

%s1 = Name of web server execution program

%s2 = Host name / IP address

Explanation

Failed to retrieve the socket information for the host name or IP address (%s2).

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

(%s1)%s2: connect to listener on %s3

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

Explanation

The communication process did not receive the daemon process completion request.

System Action

The web server stop processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: disk_cache: rename tempfile to datafile failed: %s3 -> %s4

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Temporary cache file path

%s4 = Cache file path

Explanation

Failed to update the cache file (%s4).

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

Additionally, delete all files under the directory in which the cache file that could not be updated (%s4) is stored.

(%s1)%s2: Failed to enable APR_TCP_DEFER_ACCEPT

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The socket option TCP_DEFER_ACCEPT could not be set.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: Failed to enable the '%s3' Accept Filter

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Protocol type

Explanation

Failed to optimize the socket that is listening.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: make_sock: failed to set ReceiveBufferSize for address %s3, using default

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

Explanation

The socket option ReceiveBufferSize could not be set. The socket option runs using the system default value.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: make_sock: failed to set SendBufferSize for address %s3, using default

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = IP address:Port number

Explanation

The socket option SendBufferSize could not be set. The socket option runs using the system default value.

System Action

The web server start processing is canceled.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: mpm_get_completion_context: CreateEvent failed.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The event could not be created.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

(%s1)%s2: mpm_get_completion_context: Failed to create the transaction pool.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The memory management area could not be created.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: No installed ConfigArgs for the service "%s3", using Apache defaults.

Variable Information

%s1 = Error details number

%s2 = Error details context

%s3 = Service name

Explanation

Failed to retrieve the ConfigArgs registry entry for the service (%s3).

System Action

Web server execution processing is continued.

User Action

Collect diagnostic information using the *iscollectinfo* command, and [contact your SE \(systems engineer\)](#).

(%s1)%s2: setsockopt(SO_UPDATE_ACCEPT_CONTEXT) failed.

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

The socket option could not be set.

System Action

The web server program execution processing is continued.

User Action

Check the error details number (%s1) output, and take the action described below:

Error Details Number (%s1)	Meaning / Required Action
OS 10038	The web server might have stopped when the request was received from the client - if this is the case, no action is necessary.
All other cases	Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: sigaction(%s3)**Variable Information**

%s1 = Error details number

%s2 = Error details context

%s3 = Signal type

Explanation

The signal handler could not be set.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: winnt_accept: Asynchronous AcceptEx failed.**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

The network connection was not accepted.

System Action

Web server execution processing is continued.

User Action

Check the error details number (%s1) that are output, and take the action described in the following table.

Error Details Number (%s1)	Meaning / Required Action
OS 64	A request put in a queue in the operating system was disconnected from the client - there is no need to take action. However, the request was put in the queue because the number of simultaneous connections with the client has exceeded the upper limit. If necessary, check the value set in the environment definition file (httpd.conf) ThreadsPerChild directive.
All other cases	Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: winnt_accept: Failed to allocate an accept socket. Temporary resource constraint? Try again.**Variable Information**

%s1 = Error details number

%s2 = Error details context

Explanation

A socket could not be created. Another attempt will be made in 0.1 seconds.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

(%s1)%s2: write pipe_of_death

Variable Information

%s1 = Error details number

%s2 = Error details context

Explanation

An attempt to write to the pipe failed.

System Action

Web server execution processing is continued.

User Action

Resolve the cause of the error according to the error details context (%s2).

[client %s1] handler "%s2" not found for: %s3

Variable Information

%s1 = IP address of systems such as client or proxy server

%s2 = Handler name

%s3 = File name

Explanation

The handler for the content (%s3) does not exist.

System Action

A response is given using status code "500" (Internal Server Error).

User Action

Check the MIME settings and the value set for the AddHandler/SetHandler directive in the environment definition file (httpd.conf).

default VirtualHost overlap on port %s1, the first has precedence

Variable Information

%s1 = Port number

Explanation

In the <VirtualHost> section _default_ settings in the environment definition file (httpd.conf), port number (%s1) overlaps with another host.

System Action

Web server execution processing is continued.

User Action

Check the <VirtualHost> section settings in the environment definition file (httpd.conf).

child process %s1 still did not exit, sending a SIGTERM

Variable Information

%s1 = Process ID

Explanation

SIGTERM is sent because the communication process (%s1) did not close.

System Action

Web server execution processing is aborted.

User Action

This message does not require any action.

integer overflow or out of memory condition.

Explanation

The length of the environment variable value configured in the environment definition file (httpd.conf) directives given below has exceeded 4294967295 bytes. The request is processed by treating these directive configurations as invalid.

- SetEnvIf
- SetEnvIfNoCase

System Action

Web server execution processing is continued.

User Action

Check the environment variable value configured in the environment definition file (httpd.conf). If the length of the configured environment variable value has exceeded 4294967295 bytes, reconfigure the value and ensure that this length does not exceed 4294967295 bytes.

- SetEnvIf
- SetEnvIfNoCase

Limiting internal redirects to very low numbers may cause normal requests to fail.

Explanation

The value that was set for the maximum number of internal redirects for the LimitInternalRecursion directive in the environment definition file (httpd.conf) was less than 4.

System Action

Web server execution processing is continued.

User Action

It is recommended that a value of 4 or more is set for the LimitInternalRecursion directive in the environment definition file (httpd.conf).

Limiting the subrequest depth to a very low level may cause normal requests to fail.

Explanation

The value that was set for the maximum number of subrequests for the LimitInternalRecursion directive in the environment definition file (httpd.conf) was less than 4.

System Action

Web server execution processing is continued.

User Action

It is recommended that a value of 4 or more is set for the `LimitInternalRecursion` directive in the environment definition file (`httpd.conf`).

long lost child came home! (pid %s1)

Variable Information

%s1 = Process ID

Explanation

The daemon process ended a process that was not a target for monitoring. This message is output after "graceful" is specified in the *apachectl* command and the server is restarted.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

NameVirtualHost %s1:%s2 has no VirtualHosts

Variable Information

%s1 = Virtual host name

%s2 = Port number

Explanation

The host name (%s1) set for the `NameVirtualHost` directive in the environment definition file (`httpd.conf`) is not a virtual host.

System Action

Web server execution processing is continued.

User Action

Check host name (%s1) that was set for the `NameVirtualHost` directive in the environment definition file (`httpd.conf`).

pid file %s1 overwritten -- Unclean shutdown of previous Apache run?

Variable Information

%s1 = File name

Explanation

The process ID assigned to the control process and the contents of the file (%s1) used to manage the process ID of the control process are different.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting

Explanation

The number of simultaneous connection requests from the client has exceeded the limit for the number of simultaneous connections set in the ThreadsPerChild directive in the environment definition file (httpd.conf).

Note

.....
This message is output the first time the number of requests exceeds the upper limit for the number of simultaneous connections after the web server starts up. Once this message is output, it is not output again until the web server restarts.
.....

System Action

Web server execution processing is continued.

User Action

If necessary, check the value set for the ThreadsPerChild directive in the environment definition file (httpd.conf).

SSL: The CA certificate validity term has expired.(%s1,%s2/%s3/%s4 %s5:%s6:%s7)

Variable Information

%s1 = CA certificate serial number

%s2 - %s7= CA certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

- %s2 (YYYY): Year
- %s3 (MM): Month (1 to 12)
- %s4 (DD): Date (1 to 31)
- %s5 (hh): Hour (0 to 23)
- %s6 (mm): Minute (0 to 59)
- %s7 (ss): Second (0 to 59)

Explanation

The validity term of the CA certificate has expired.

If a web server operation is continued even though the CA certificate's validity term has already expired, the following problems will occur:

- Communication with the client fails.
- The web server cannot be restarted.

Web server execution processing is continued.

User Action

Take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new CA certificate.
2. Reregister a new CA certificate.
3. Restart the web server.

SSL: The CA certificate will expire in %s1 days.(%s2,%s3/%s4/%s5 %s6:%s7:%s8)

Variable Information

%s1 = Number of days left until the CA certificate's validity term will expire

%s2 = CA certificate serial number

%s3 -%s8= CA certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

- %s3 (YYYY): Year
- %s4 (MM): Month (1 to 12)
- %s5 (DD): Date (1 to 31)
- %s6 (hh): Hour (0 to 23)
- %s7 (mm): Minute (0 to 59)
- %s8 (ss): Second (0 to 59)

Explanation

The validity term of the CA certificate will expire in %s1 days.

System Action

Web server execution processing is continued.

User Action

Before the validity term of the CA certificate expires, take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new CA certificate.
2. Reregister a new CA certificate.
3. Restart the web server.

SSL: The site certificate validity term has expired.(%s1,%s2/%s3/%s4 %s5:%s6:%s7)

Variable Information

%s1 = site certificate nickname

%s2 -%s7 = site certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

- %s2 (YYYY): Year
- %s3 (MM): Month (1 to 12)
- %s4 (DD): Date (1 to 31)
- %s5 (hh): Hour (0 to 23)
- %s6 (mm): Minute (0 to 59)
- %s7 (ss): Second (0 to 59)

Explanation

The validity term of the site certificate (%s1) has expired.

If a web server operation is continued even though the site certificate's validity term has already expired, the following problems will occur:

- Communication with the client fails.
- The web server cannot be restarted.

System Action

Web server execution processing is continued.

User Action

Take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new site certificate.
2. Reregister a new site certificate.
3. Restart the web server.

SSL: The site certificate will expire in %s1 days.(%s2,%s3/%s4/%s5 %s6:%s7:%s8)

Variable Information

%s1 = Number of days left until the site certificate's validity term will expire

%s2 = site certificate nickname

%s3 - %s8 = site certificate validity term (Format: "YYYY/MM/DD hh:mm:ss")

- %s3 (YYYY): Year

- %s4 (MM): Month (1 to 12)

- %s5 (DD): Date (1 to 31)

- %s6 (hh): Hour (0 to 23)

- %s7 (mm): Minute (0 to 59)

- %s8 (ss): Second (0 to 59)

Explanation

The validity term of the site certificate (%s2) will expire in %s1 days.

System Action

Web server execution processing is continued.

User Action

Before the validity term of the site certificate expires, take action according to the following procedure:

1. Make a request to the CA (certificate issuer) to issue a new site certificate.
2. Reregister a new site certificate.
3. Restart the web server.

VirtualHost %s1:%s2 overlaps with VirtualHost %s3:%s4, the first has precedence, perhaps you need a NameVirtualHost directive

Variable Information

%s1 = Virtual host name

%s2 = Port number

%s3 = Virtual host name

%s4 = Port number

Explanation

In the <VirtualHost> section settings in the environment definition file (httpd.conf), the virtual host name and port number overlap.

System Action

Web server execution processing is continued.

User Action

Check the <VirtualHost> section settings in the environment definition file (httpd.conf).

WARNING: Attempt to change ServerLimit or ThreadLimit ignored during restart

Explanation

The ServerLimit directive or the ThreadLimit directive settings in restart are ignored. The ServerLimit directive and the ThreadLimit directive use the values set during the previous startup.



Change the value set for the ServerLimit and ThreadLimit directives after stopping the web server.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

WARNING: Attempt to change ThreadLimit ignored during restart

Explanation

The ThreadLimit directive settings in restart are ignored.

System Action

Web server execution processing is continued.

User Action

This message does not require any action.

8.10.6 Messages Whose Log Levels are "notice"

The meaning and user action for log level "notice" is explained.

Message list

1. %s1 configured -- resuming normal operations
2. cannot use a full URL in a 401 ErrorDocument directive --- ignoring!
3. caught SIGTERM, shutting down
4. caught SIGWINCH, shutting down gracefully
5. Child %s1: Acquired the start mutex.
6. Child %s1: All worker threads have exited.
7. Child %s1: Child process is exiting
8. Child %s1: Child process is running
9. Child %s1: Exit event signaled. Child process is ending.

10. Child %s1: Process exiting because it reached MaxRequestsPerChild. Signaling the parent to restart a new child process.
11. Child %s1: Released the start mutex
12. Child %s1: Starting %s2 worker threads.
13. Child %s1: Starting thread to listen on port %s2.
14. Child %s1: Terminating %s2 threads that failed to exit.
15. Child %s1: Waiting %s2 more seconds for %s3 worker threads to finish.
16. child pid %s1 exit signal %s2 (%s3)
17. child pid %s1 exit signal %s2 (%s3), possible coredump in %s4
18. Disabled use of AcceptEx() WinSock2 API
19. Parent: Child process exited successfully.
20. Parent: child process exited with status %s1 -- Restarting.
21. Parent: Created child process %s1
22. Parent: Forcing termination of child process %s1
23. Parent: Received restart signal -- Restarting the server.
24. Parent: Received shutdown signal -- Shutting down the server.
25. seg fault or similar nasty error detected in the parent process
26. Server built: %s1
27. SIGHUP received. Attempting to restart
28. SIGUSR1 received. Doing graceful restart

Explanation and User action of Messages

%s1 configured -- resuming normal operations

Variable Information

%s1 = Server information

Explanation

Initialization processing was completed normally.

cannot use a full URL in a 401 ErrorDocument directive --- ignoring!

Explanation

An external URL cannot be specified in the error document if status code "401" is specified for the ErrorDocument directive in the environment definition file (httpd.conf). The ErrorDocument directive settings in the environment definition file (httpd.conf) are disabled.

Note

.....
 User authentication cannot be used because the client cannot accept status code "401".

System Action

Web server execution processing is continued.

User Action

If status code "401" is specified for the ErrorDocument directive in the environment definition file (httpd.conf), specify the text message or internal URL in the error document.

caught SIGTERM, shutting down

Explanation

The daemon process has received the SIGTERM signal, therefore the web server stop processing will start.

caught SIGWINCH, shutting down gracefully

Explanation

The daemon process has received the SIGWINCH signal, therefore the web server stop processing will start.

Child %s1: Acquired the start mutex.

Variable Information

%s1 = Process ID of the daemon process

Explanation

Exclusive resources were acquired.

Child %s1: All worker threads have exited.

Variable Information

%s1 = Process ID of the daemon process

Explanation

All communication threads have closed.

Child %s1: Child process is exiting

Variable Information

%s1 = Process ID of the daemon process

Explanation

The daemon process is stopping.

Child %s1: Child process is running

Variable Information

%s1 = Process ID of the daemon process

Explanation

The daemon process is starting.

Child %s1: Exit event signaled. Child process is ending.

Variable Information

%s1 = Process ID of the daemon process

Explanation

A stop event was received. The daemon process (%s1) starts close processing.

Child %s1: Process exiting because it reached MaxRequestsPerChild. Signaling the parent to restart a new child process.

Variable Information

%s1 = Process ID of the daemon process

Explanation

The daemon process is restarted because the number of requests processed in daemon process (%s1) has reached the value set for the MaxRequestsPerChild directive in the environment definition file (httpd.conf).

Child %s1: Released the start mutex

Variable Information

%s1 = Process ID of the daemon process

Explanation

Exclusive resources were released.

Child %s1: Starting %s2 worker threads.

Variable Information

%s1 = Process ID of the daemon process

%s2 = The value set for the ThreadsPerChild directive in the environment definition file (httpd.conf)

Explanation

Communication threads are created.

Child %s1: Starting thread to listen on port %s2.

Variable Information

%s1 = Process ID of the daemon process

%s2 = The number of communication threads that could not close

Explanation

The listener thread started processing.

Child %s1: Terminating %s2 threads that failed to exit.

Variable Information

%s1 = Process ID of the daemon process

%s2 = The number of communication threads that could not close

Explanation

The communication threads were stopped by force because they could not stop within the allowed time.

Child %s1: Waiting %s2 more seconds for %s3 worker threads to finish.

Variable Information

%s1 = Process ID of the daemon process

%s2 = Wait time until the threads complete

%s3 = Number of communication threads that the daemon process is waiting to complete

Explanation

The daemon process waits for the communication threads to complete.

child pid %s1 exit signal %s2 (%s3)

Variable Information

%s1 = Process ID of the communication process

%s2 = Error details context

%s3 = Received signal number

Explanation

Signal (%s3) was received in communication process (%s1).

User Action

If the error details context (%s2) is "Segmentation fault" and there is no response to any of the requests that used a web server connector, the web server connector operations may become unstable due to instances of insufficient disk space in the past.

Refer to the event log (Windows(R)) or the system log (Solaris/Linux) to check if there is sufficient disk space. If an instance of insufficient disk space did occur, check if the web server was restarted after the occurrence. If the web server was not restarted, secure the required disk space and restart the web server.

child pid %s1 exit signal %s2 (%s3), possible coredump in %s4

Variable Information

%s1 = Process ID of the communication process

%s2 = Error details context

%s3 = Received signal number

%s4 = Output core file name

Explanation

A signal (%s3) was received in the communication process (%s1). The core file (%s4) is output.

Disabled use of AcceptEx() WinSock2 API

Explanation

The Win32DisableAcceptEx directive has been configured.

Parent: Child process exited successfully.

Explanation

The daemon process closed normally.

Parent: child process exited with status %s1 -- Restarting.

Variable Information

%s1 = Daemon process exit code

Explanation

The daemon process is restarted.

Parent: Created child process %s1

Variable Information

%s1 = Process ID of the daemon process

Explanation

The daemon process was created.

Parent: Forcing termination of child process %s1

Variable Information

%s1 = Daemon process handle number

Explanation

The daemon process could not be closed within the allowed time. The corresponding process is closed by force.

Parent: Received restart signal -- Restarting the server.

Explanation

The web server restart processing is started.

Parent: Received shutdown signal -- Shutting down the server.

Explanation

The web server stop processing is started.

seg fault or similar nasty error detected in the parent process

Explanation

- The monitoring process received one of the following signals:
- SIGSEGV
- SIGBUS
- SIGABORT
- SIGABRT
- SIGILL

Server built: %s1

%Variable Information

%s1 = Build time

Explanation

This is the compile time.

SIGHUP received. Attempting to restart

Explanation

The daemon process has received the SIGHUP signal, therefore the web server restart processing will start.

SIGUSR1 received. Doing graceful restart

Explanation

The daemon process has received the SIGUSR1 signal, therefore the web server restart processing will start.

Chapter 9 Troubleshooting

This chapter explains the action to take if a problem occurs while Interstage HTTP Server 2.2 is running.

For errors that occur during operations in Interstage HTTP Server 2.2, the error is written to an event log in Windows(R) systems, and a message is written to a system log in Solaris/Linux systems. Refer to "[Chapter 8 Messages](#)", and follow the corrective action advised for the message.

Additionally, access logs, error logs, and trace logs are also output. For details on the logs, refer to "[4.2 Log](#)".

Here, case studies of problems that have occurred while Interstage HTTP Server 2.2 was running, and the corrective actions, are explained.

9.1 Errors when the Web Server Starts or Stops

This section explains the action to take if a problem occurs when the web server starts or stops.

The web server is stopped during the Apache HTTP Server operation Linux32/64

In RHEL5(x86)/RHEL5(Intel64), if Apache HTTP Server (httpd bundled with the basic software) is stopped, the web server may also stop.

If the Apache HTTP Server shell (/etc/rc.d/init.d/httpd) is executed to stop Apache HTTP Server, it will end all processes with the process name "httpd". Therefore, because web server processes with the process name "httpd" are also ended, this will cause the web server to stop.

If this problem occurs, take one of the following actions:

- Migrate Apache HTTP Server to a package of httpd-2.2.3-43.el5 or later before running it. Note that, when Apache HTTP Server is uninstalled, the shell (/etc/rc.d/init.d/httpd) is also executed, therefore the same problem will occur.
- To stop Apache HTTP Server, use the Apache HTTP Server apachectl command. For details on how to stop the Apache HTTP Server using the apachectl command, refer to the documentation for the Apache HTTP Server used.

9.2 Errors During Web Server Operation

This section explains the action to take if a problem occurs during web server operation.

- [There is no response from the web server or the response from the web server is delayed](#)
- [No log file is output](#)
- [When accessing from a web browser, an unintended page is displayed](#)



See

.....
For details on the web application error, refer to "Troubleshooting" in the "Java EE Operator's Guide (Java EE 6 Edition)".
.....

There is no response from the web server or the response from the web server is delayed

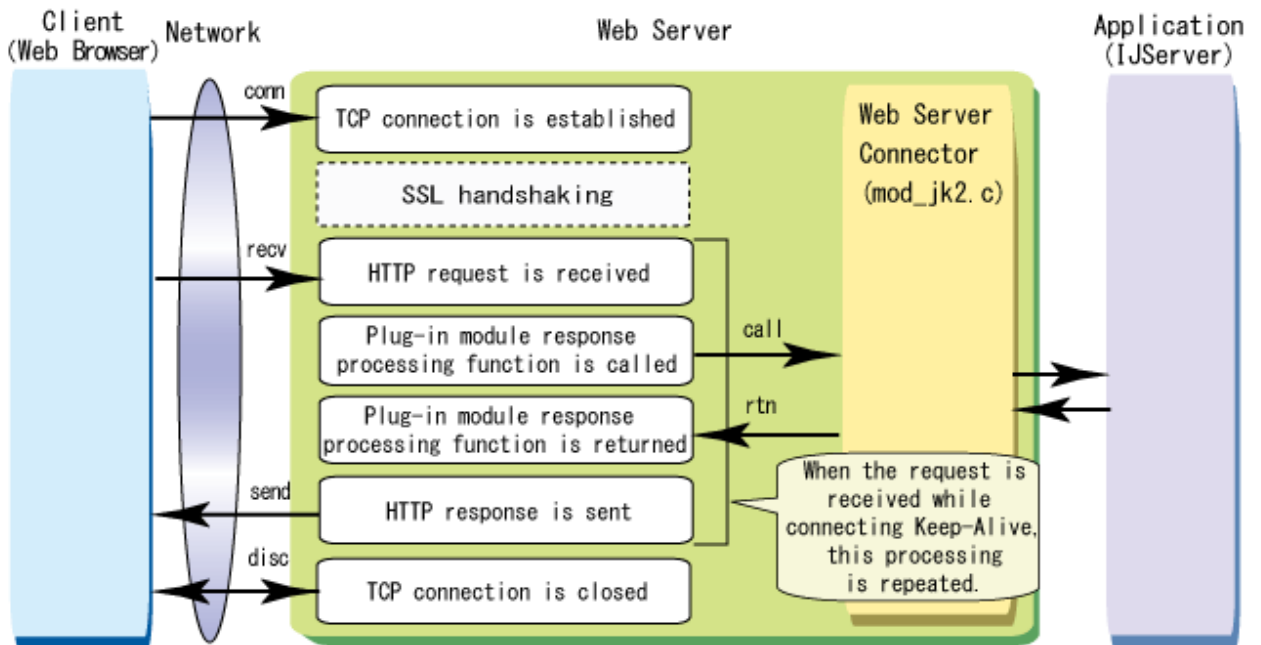
If this issue occurs, check whether there is a problem and then take action according to the following procedure.

Procedure

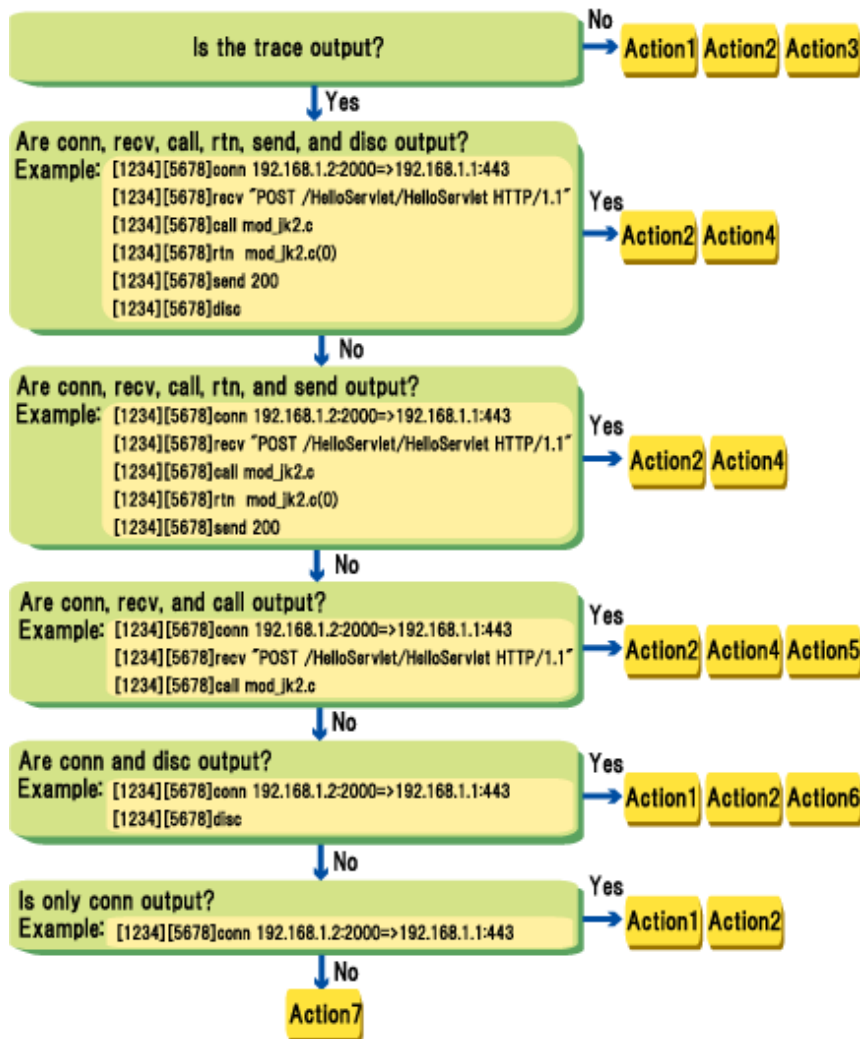
Refer to the trace log, and check whether there is a problem from the output content for the trace information of the period during which the issue occurred. For details on the trace log, refer to "[4.2.3 Trace Log](#)".

1. Extract the output for the trace log events (conn, recv, call, rtn, send, disc) using the method shown below. For details on the event output flow, refer to the figure shown below.

The trace information is extracted as a combination of the same process ID and thread ID. If you know the client IP address when this issue occurs, extract the thread ID of the conn event to which that client IP address is output.



2. Refer to the figure shown below, and then take action according to the output content for the trace information that was extracted in 1.



Action 1

The request may not have reached the web server.
Check whether the request data has been sent from the client.

Action 2

A delay may have occurred on the network device (router or load balancer, for example) between the request sender client and the destination web server.
Check whether the network device (router or load balancer, for example) between the client and the web server is running normally.

Action 3

The trace log of the period during which the problem occurred may have been deleted by the log rotation function.
Check the upper limit values for the trace log file size and the number of files. For details on the setting the trace log, refer to "3.6 Setting the Trace Log".

Action 4

If any of the following conditions is apparent in the output content for the trace information, the Servlet service application processing may be delayed.

Check whether a problem has occurred in the web server connector and the application.

- rtn events are not output after call events
- There is a big time difference between call events and rtn events

Action 5

For POST requests, the body data from the client may not have arrived.

Check whether the POST request body data has been sent from the client.

Action 6

In SSL communication, the SSL handshake may have failed.

Check whether an error log has been output. If it has, remove the cause of the error in the message. For details on the error log, refer to "8.10 Error Log".

Action 7

Collect diagnostic information with the *iscollectinfo* command, and then [contact your systems engineer](#).

No log file is output

If this issue occurs, the most recent log file may have been operated on by mistake. The most recent log file cannot be operated on, using edit or delete for example, while the web server is running. If the most recent log file is operated on by mistake, restart the web server.

When accessing from a web browser, an unintended page is displayed

If this issue has occurred, the Interstage HTTP Server 2.2 port number (default value: 80) and the port number of another web server (for example, Apache HTTP Server which is bundled with the basic software) may be duplicated.

If the web servers are being operated alongside each other, you must set different port numbers for each of them.

If the other web server was started using the same port number, change the Interstage HTTP Server 2.2 port number and then restart the web server. For details on the setting the port number, refer to "3.3 Setting the Port Number and IP Address".

9.3 Errors When Multiple Web Servers are Used

This section explains the action to take if a problem occurs while the web server operating environment is being created.

- [When registering the web server service, the service name displayed in the message is erroneous and garbled](#) [Windows32/64](#)
- [When registering the web server service, Usage of the httpd command is output after the message](#) [Windows32/64](#)

When registering the web server service, the service name displayed in the message is erroneous and garbled [Windows32/64](#)

When registering the service using the httpd command, if the message shown below is output and the service name that was registered is erroneous and garbled, a service name containing double-byte characters may have been specified for the service name that was registered.

Example of the execution for registering the service

```
C:\Interstage\F3FMahs\bin\httpd.exe -k install -n "service name" -f "<directory containing the web server resources>\conf\httpd.conf"
```

Messages

```
Installing the <erroneous service name> service
The <erroneous service name> service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
```

Service names containing double-byte characters cannot be registered as web server service names.

If this issue occurs, delete the erroneous service that was registered, specify the httpd command option correctly, and then register the web server service again.

The procedure used to delete the erroneous service that was registered is shown below.

1. Log in with Administrator privileges.
2. Open the registry editor.
3. Move to the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

4. Delete the key for the service name containing double-byte characters specified when the service was registered.
5. Search for the erroneous service name key that was registered. Identify the erroneous service name by checking the data, shown below, in which the service name has been registered.

Note) The erroneous service name identified here may be different to the erroneous service name output to the message.

Name	kind	Data
ImagePath	REG_EXPAND_SZ	"C:\Interstage\F3FMahs\bin\httpd.exe" -k runservice

6. Execute the following command to delete the erroneous service name identified in 5:

```
sc delete "erroneous service name"
```

When registering the web server service, usage of the httpd command is output after the message

Windows32/64

When registering the service using the httpd command, if usage of the httpd command is output after the message shown below, the service may have been registered using wrong options of the httpd command by mistake.

If this issue occurs, delete the service that was registered, specify the [httpd](#) command option correctly, and then register the web server service again.

Messages

```
Installing the <service name> service
The <service name> service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
(Note)
```


Note) The error details may be displayed.

9.4 Errors When the Cluster Service Function is Used

This section explains the action to take when an error occurs using the cluster service function.

The web server fails to start Windows32/64

When using the cluster service function, the following message is written to the system log of the event viewer and the web server may fail to start:

```
Interstage HTTP Sever 2.2(Note) service terminated with service-specific error 1 (0x1).
```

Note) The Interstage HTTP Server 2.2 service name is output for the registered resources.

If this issue occurs, take the following action shown below.

- In Windows Server(R) 2008, execute the following command to delete the setup parameters:

```
Cluster Resource "resource name" /priv StartupParameters=""
```

- In Windows Server(R) 2012, using the failover cluster manager, open the [Properties]-[General] tabs of the registered resource, and then delete "startup parameters".

9.5 Frequently Asked Questions and Solutions

Frequently asked questions and solutions relating to Interstage HTTP Server 2.2 operations are shown below.

- [Is there support for the security hole-related problem in Apache HTTP Server Version 2.2.22?](#)
- [Can multiple web servers be started?](#)
- [Can Interstage HTTP Server 2.2 and other web servers \(for example, Apache HTTP Server\) coexist?](#)
- [Can certificates issued using OpenSSL be used?](#)
- [Are third-party plug-in modules supported?](#)
- [Which HTTP methods can be used for static content?](#)
- [For access from the web browser, "It works!" is displayed](#)

Is there support for the security hole-related problem in Apache HTTP Server Version 2.2.22?

The fix for the security hole detected in Apache HTTP Server Version 2.2 that affects Interstage HTTP Server 2.2 is effective for versions up to Apache HTTP Server Version 2.2.25. Additionally, if a problem related to a security hole occurs after this product is shipped, it will be fixed as needed by an urgent patch.

Security information on Fujitsu products is available from the following site. Keep checking the latest information.

```
http://software.fujitsu.com/jp/security/index.html
```

Can multiple web servers be started?

In Interstage HTTP Server 2.2, multiple web servers can be built and operated on one system.



See

For details on creating and deleting, refer to "4.3 Multiple Web Server Operation".

Can Interstage HTTP Server 2.2 and other web servers (for example, Apache HTTP Server) coexist?

Interstage HTTP Server 2.2 and other web servers (for example, Apache HTTP Server) can coexist. However, the same port number cannot be used on multiple web servers. A different port number must be set for each web server.

Can certificates issued using OpenSSL be used?

Certificates issued using OpenSSL cannot be used in Interstage HTTP Server 2.2.



See

For details on the certificate, refer to the following paragraphs of the Security System Guide.

- To use Interstage Certificate Environment SSL communication:
"Setting and Use of the Interstage Certificate Environment" chapter
- To use SSL communication in the certificate/key management environment that is built using the SMEE command:
"Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter

Are third-party plug-in modules supported?

In Interstage HTTP Server 2.2, third-party plug-in modules, including mod_perl and mod_php, are not supported. Only the plug-in modules that are provided in the Fujitsu product can be used.

Note that, if the plug-in module that is installed is not supported in Interstage HTTP Server 2.2, none of the Interstage HTTP Server 2.2 operations will be supported either.

Which HTTP methods can be used for static content?

In Interstage HTTP Server 2.2, the HTTP methods shown below can be used for static content. The POST method cannot be used.

- GET
- HEAD
- OPTIONS
- TRACE

For access from the web browser, "It works!" is displayed

If "It works!" is displayed for access from the web browser, a sample file provided in Interstage HTTP Server 2.2 will be displayed.

This sample file is stored as follows. Replace this file according to the operation, before starting the web server operation.

Windows32/64

```
C:\Interstage\F3FMahs\htdocs\index.html
```

Solaris32/64 Linux32/64

```
/opt/FJSVahs\htdocs/index.html
```

Chapter 10 Migrating to Interstage HTTP Server 2.2

The functions shown below provided in Interstage Application Server cannot be migrated from the web server to Interstage HTTP Server 2.2 (web server based on Apache HTTP Server Version 2.2).

To use these web server functions in Interstage HTTP Server 2.2, install Interstage HTTP Server 2.2 and then edit the environment definition file (httpd.conf) directly and configure the required functions. For details on configuring the Interstage HTTP Server 2.2 operating environment, refer to "[Chapter 3 Configuring the Web Server Operating Environment](#)".

- Interstage HTTP Server in this version or earlier (based on Apache HTTP Server Version 2.0)
- Interstage HTTP Server 8.0 or earlier (based on Apache HTTP Server Version 1.3)
- InfoProvider Pro V7.0 or earlier



Linux32/64

When using CGI programs in Interstage HTTP Server 2.2, the behavior will be different to the behavior on the above web servers. For details, refer to "[4.9 Notes](#)" - "[CGI Programs](#)".

Appendix A Miscellaneous Information

This appendix explains miscellaneous Interstage HTTP Server 2.2 information.


A.1 Log Files

This log information output in Interstage HTTP Server 2.2 is shown below.



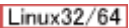

Usage	Default output	Default file name	Default path	Default size x Number of generations
Access Log of the Interstage HTTP Server 2.2	Yes	accesslog accesslog.N (N is a serial number from 0 to 999.)	Windows32/64 C:\Interstage\F3FMahs\logs\ Solaris32/64 Linux32/64 /var/opt/FJSVahs/logs/	1 MB * 5
Error Log of the Interstage HTTP Server 2.2	Yes	errorlog errorlog.N (N is a serial number from 0 to 999.)		1 MB * 5
Trace Log of the Interstage HTTP Server 2.2	Yes	tracelog tracelog.N (N is a serial number from 0 to 999.)		2 MB * 5

Access Log of Interstage HTTP Server 2.2




Default Output	Yes
Default File Name	accesslog, accesslog.N (N is a serial number from 0 to 999.)
Default Path	Windows32/64 C:\Interstage\F3FMahs\logs\ Solaris32/64 Linux32/64 /var/opt/FJSVahs/logs/
Number of Generations	Default: 5; Maximum: 999
Size	Default: 1 MB; Maximum: 2047 MB
Length of Record	Variable
Condition for Rotation	When the log file is updated from the log output, if the maximum file size specified is exceeded, the old information changes to "accesslog.N". In the default setting, rotation is set in units of file size. However, rotation can also be set in units of time/date/days of week/number of days.
Reference in the Manuals	"4.2.1 Access Log"
Location of Settings	The log file name, path, and output items are set in the CustomLog directive of the environment definition file (httpd.conf).
Collection target when iscollectinfo is used?	Yes


	 Note <p>If the log file output destination is changed from the default path, it will not be a collection target. In this case, collect the log files separately.</p>
Remarks	This outputs the access status from the web client.

Error Log of Interstage HTTP Server 2.2

Default Output	Yes
Default File Name	errorlog, errorlog.N (N is a serial number from 0 to 999.)
Default Path	 C:\Interstage\F3FMahs\logs\   /var/opt/FJSVahs/logs/
Number of Generations	Default: 5;, Maximum: 999
Size	Default: 1 MB; Maximum: 2047 MB
Length of Record	Variable
Condition for Rotation	When the log file is updated from the log output, if the maximum file size specified is exceeded, the old information changes to "errorlog.N". In the default setting, rotation is set in units of file size. However, rotation can also be set in units of time/date/days of week/number of days.
Reference in the Manuals	"4.2.2 Error Log"
Location of Settings	The log file name, path, and output items are set in the ErrorLog directive of the environment definition file (httpd.conf).
Collection target when iscollectinfo is used?	Yes  Note <p>If the log file output destination is changed from the default path, it will not be a collection target. In this case, collect the log files separately.</p>
Remarks	If an error occurs in Interstage HTTP Server 2.2, an error message is output.

Trace Log of Interstage HTTP Server 2.2

Default Output	Yes
Default File Name	tracelog, tracelog.N (N is a serial number from 0 to 999.)
Default Path	 C:\Interstage\F3FMahs\logs\   /var/opt/FJSVahs/logs/
Number of Generations	Default: 5; Maximum: 999
Size	Default: 2 MB; Maximum: 2047 MB
Length of Record	Variable

Condition for Rotation	When the log file is updated from the log output, if the maximum file size specified is exceeded, the old information changes to "tracelog.N". In the default setting, rotation is set in units of file size. However, rotation can also be set in units of time/date/days of week/number of days.
Reference in the Manuals	"4.2.3 Trace Log"
Location of Settings	The log file name, path, and output items are set in the TraceLog directive of the environment definition file (httpd.conf).
Collection target when iscollectinfo is used?	Yes  Note If the log file output destination is changed from the default path, it will not be a collection target. In this case, collect the log files separately.
Remarks	The web client and plug-in module I/O information is output.

A.2 Port Numbers

For ports used by Interstage Application Server, a different port number must be set for each service. If the same port number is set and the service is then run, the behavior will not be normal. For example, access from the client will not be possible.

The port numbers used in Interstage HTTP Server 2.2 are shown below. If any of these port numbers are already being used in Interstage HTTP Server 2.2, reset the port number.

Usage	Port number/Protocol
Port Number of Interstage HTTP Server 2.2	80/tcp (This can be changed.)
Port Number of the Virtual Host	Unused port number between 1 and 65535/tcp
Port Number Used in Communication with the Transfer Destination when the Proxy Function is Used	Undefined/tcp

Port Number of Interstage HTTP Server 2.2

Fixed/Undefined	Fixed
Port number/Protocol	80/tcp (This can be changed.)
Reference in the Manuals	"3.3 Setting the Port Number and IP Address"
Location of the port number setting	The port number is set in the Listen directive of the environment definition file (httpd.conf).
Remarks	In the web server, the following port numbers are normally used: - HTTP(when SSL is not used): 80 (Note) - HTTPS(when SSL is used): 443

Note)   

In the Web Package, if the port number is not specified during the installation, port number "8180" will be used for the installation.

Port Number of the Virtual Host

Fixed/Undefined	Fixed
Port number/Protocol	Unused port number between 1 and 65535/tcp
Reference in the Manuals	" 3.11 Setting the Virtual Host "
Location of the port number setting	The port number is set in the Listen directive, the NameVirtualHost directive, and the <VirtualHost> section of the environment definition file (httpd.conf).
Remarks	None

Port Number Used in Communication with the Transfer Destination when the Proxy Function is Used

Fixed/Undefined	Undefined
Port number/Protocol	Undefined/tcp
Reference in the Manuals	None
Location of the port number setting	None
Remarks	When the proxy function is used, an ephemeral port is automatically assigned for the port number used.

A.3 Resident Processes

This section explains the resident processes required in monitoring in Interstage HTTP Server 2.2.



Process names

Windows32/64

"C:\Interstage" is the Interstage Application Server installation path. This may change according to the actual installation environment that is used.


Solaris32/64 Linux32/64

This is the output result for the "ps -ef" command.

Clustering

When clustering is used for operations, it will be explained whether monitoring of the corresponding processes in the process monitoring software is required.

Process Name	<p>Windows32/64</p> <p>C:\Interstage\F3FMahs\bin\httpd.exe</p> <p>Solaris32/64 Linux32/64</p> <p>/opt/FJSVahs/bin/httpd</p>
Number of Processes	Number of web servers x 1

	 Note <p>Multiple processes are started, however, you should monitor only processes having process IDs defined in the process management files shown below. Note that these process management files exist only while the web server is running.</p> <p>Windows32/64</p> <p>C:\Interstage\F3FMahs\logs\httpd.pid</p> <p>Solaris32/64 Linux32/64</p> <p>/opt/FJSVahs/logs/httpd.pid</p>
Functionality Overview	<p>Windows32/64</p> <p>This is the Interstage HTTP Server 2.2 start process. It monitors the daemon processes.</p> <p>Solaris32/64 Linux32/64</p> <p>This is the Interstage HTTP Server 2.2 daemon process. It monitors the communication processes.</p>
Residency	If Interstage HTTP Server 2.2 is used, the process will stay resident.
Process monitoring	Required
Clustering	Not required
Explanation about monitoring	If the corresponding process has abended, it will be necessary to monitor using the process monitoring software, because there is no procedure for automatic startup. However, if the corresponding process abends while the cluster is running, it will not be necessary to use the process monitoring software, because the active node and standby node will switch.
Remarks	When multiple web servers are running, processes will have to be monitored for each web server.
Start command/Stop command	For starting the web servers, refer to " 4.1.1 Starting the Web Server ". For stopping the web servers, refer to " 4.1.2 Stopping the Web Server ".

A.4 Messages

This section explains the messages that must be monitored in Interstage HTTP Server 2.2.

A.4.1 Event Log **Windows32/64**

The messages that must be monitored are output to an event log.

To monitor errors notified in Interstage HTTP Server 2.2 using a monitoring tool, for example, monitor the event log error messages based on the information shown below.

Specific Error Message Information

Log type	Source name	Monitoring condition
Application	AHS	Error type is not "INFO"

A.4.2 syslog Solaris32/64 Linux32/64

The messages that must be monitored are output to a syslog.

To monitor errors notified in Interstage HTTP Server 2.2 using a monitoring tool, for example, monitor the syslog error messages based on the information shown below.

Output Directory

Solaris32/64

```
/var/adm/messages
```

Linux32/64

```
/var/log/messages
```

Output Format

```
Label: Error type: Message text
```

Label/ Message ID	Error type	Message text
UX:AHS	"INFO"	Any string
	"WARNING"	
	"ERROR"	

Output Example

```
UX:AHS: ERROR: ahs00004: Pre-configuration failed [%s]
```

Output Message Facility and Priority (level)

Facility	Error Type	Priority (level)
daemon	"INFO"	info notice
	"WARNING"	notice warn warning
	"ERROR"	err error crit alert emerg

Appendix B Environment Variables and Server Variables

This appendix explains the environment variables and server variables used in Interstage HTTP Server 2.2.

Note

The environment variables and server variables explained here can be used internally in Interstage HTTP Server 2.2.

Environment Variables

The environment variables are used as shown below. Note that these are not the same as the environment variables that are controlled in the operating system. However, if they are passed to a CGI program or SSI page, they can be used as operating system environment variables.

- [Access Control](#) (Allow, Deny)
- [Access Log Output](#) (CustomLog, LogFormat)
- [HTTP Response Header Control](#) (Header)
- [URL Rewrite](#) (RewriteCond, RewriteRule)

Point

Settings for any environment variable

Any environment variable can be set using the following directives:

- BrowserMatch
- BrowserMatchNoCase
- [RewriteRule](#) (flag "env=environment variable:value" or "E= environment variable:value")
- SetEnvIf
- SetEnvifNoCase

Access Control

Access control is performed according to the value set for the environment variable.

The directives that can be used by the environment variables, the environment variables that can be specified in those directives and the requests that can be used by those environment variables are shown below. For details on the environment variables, refer to "[List of Variables](#)".

Directive that can be used	Environment variable that can be specified	Request that can be used
<ul style="list-style-type: none">- Allow- Deny	<ul style="list-style-type: none">- UNIQUE_ID (Note 1)- HTTPS- HTTPS_CIPHER (Note 2)- HTTPS_SECRETKEYSIZE (Note 2)- SSL_CLIENT_CN (Note 2)(Note 3)	<ul style="list-style-type: none">- Static content- CGI program- Servlet service application

Directive that can be used	Environment variable that can be specified	Request that can be used
	<ul style="list-style-type: none"> - SSL_CLIENT_C (Note 2)(Note 3) - SSL_CLIENT_EMAIL (Note 2)(Note 3) - SSL_CLIENT_O (Note 2)(Note 3) - SSL_CLIENT_OU (Note 2)(Note 3) - SSL_CLIENT_T (Note 2)(Note 3) - SSL_CLIENT_PHONE (Note 2)(Note 3) - SSL_CLIENT_ST (Note 2)(Note 3) - SSL_CLIENT_L (Note 2)(Note 3) - Arbitrary environment variable 	

Note 1) The module "mod_unique_id" must be set in the LoadModule directive.

Note 2) The SSLNotifyVers directive must be set to "On". Optional (default: On).

Note 3) The SSLCertExpand directive must be set to "On". Optional (default: On).

Access Log Output

Access log output is controlled according to the value set for the environment variable. Additionally, the value set for the environment variable is output to the access log.

The directives that can be used by the environment variables, the environment variables that can be specified in those directives and the requests that can be used by those environment variables are shown below. For details on the environment variables, refer to "List of Variables".

Directive that can be used	Environment variable that can be specified	Request that can be used
<ul style="list-style-type: none"> - CustomLog - LogFormat 	<ul style="list-style-type: none"> - UNIQUE_ID (Note 1) - HTTPS - HTTPS_CIPHER (Note 2) - HTTPS_SECRETKEYSIZE (Note 2) - SSL_CLIENT_CN (Note 2)(Note 3) - SSL_CLIENT_C (Note 2)(Note 3) - SSL_CLIENT_EMAIL (Note 2)(Note 3) - SSL_CLIENT_O (Note 2)(Note 3) - SSL_CLIENT_OU (Note 2)(Note 3) - SSL_CLIENT_T (Note 2)(Note 3) - SSL_CLIENT_PHONE (Note 2)(Note 3) 	<ul style="list-style-type: none"> - Static content - CGI program - Servlet service application

Directive that can be used	Environment variable that can be specified	Request that can be used
	<ul style="list-style-type: none"> - SSL_CLIENT_ST (Note 2)(Note 3) - SSL_CLIENT_L (Note 2)(Note 3) - Arbitrary environment variable 	
	<ul style="list-style-type: none"> - HTTP_USER_AGENT - HTTP_REFERER - HTTP_COOKIE - HTTP_FORWARDED - HTTP_HOST - HTTP_PROXY_CONNECTION - HTTP_ACCEPT - CONTENT_TYPE - CONTENT_LENGTH - REMOTE_ADDR - REMOTE_PORT - REMOTE_HOST - REMOTE_USER - REMOTE_IDENT - AUTH_TYPE - DOCUMENT_ROOT - SERVER_ADMIN - SERVER_NAME - SERVER_ADDR - SERVER_PORT - SERVER_SIGNATURE - SERVER_SOFTWARE 	<ul style="list-style-type: none"> - CGI program - Servlet service application
	<ul style="list-style-type: none"> - REQUEST_METHOD - REQUEST_URI - GATEWAY_INTERFACE - SCRIPT_NAME - SCRIPT_FILENAME - SERVER_PROTOCOL - PATH_INFO - PATH_TRANSLATED - QUERY_STRING 	<ul style="list-style-type: none"> - CGI program

Note 1) The module "mod_unique_id" must be set in the LoadModule directive.

Note 2) The [SSLNotifyVers](#) directive must be set to "On". Optional (default: On).

Note 3) The [SSLCertExpand](#) directive must be set to "On". Optional (default: On).

HTTP Response Header Control

The HTTP response header is controlled according to whether the environment variable exists.

The directives that can be used by the environment variables, the environment variables that can be specified in those directives and the requests that can be used by those environment variables are shown below. For details on the environment variables, refer to "[List of Variables](#)".

Directive that can be used	Environment variable that can be specified	Request that can be used
- Header	<ul style="list-style-type: none"> - UNIQUE_ID (Note 1) - HTTPS - HTTPS_CIPHER (Note 2) - HTTPS_SECRETKEYSIZE (Note 2) - SSL_CLIENT_CN (Note 2)(Note 3) - SSL_CLIENT_C (Note 2)(Note 3) - SSL_CLIENT_EMAIL (Note 2)(Note 3) - SSL_CLIENT_O (Note 2)(Note 3) - SSL_CLIENT_OU (Note 2)(Note 3) - SSL_CLIENT_T (Note 2)(Note 3) - SSL_CLIENT_PHONE (Note 2)(Note 3) - SSL_CLIENT_ST (Note 2)(Note 3) - SSL_CLIENT_L (Note 2)(Note 3) - Arbitrary environment variable 	<ul style="list-style-type: none"> - Static content - CGI program - Servlet service application
	<ul style="list-style-type: none"> - HTTP_USER_AGENT - HTTP_REFERER - HTTP_COOKIE - HTTP_FORWARDED - HTTP_HOST - HTTP_PROXY_CONNECTION - HTTP_ACCEPT - CONTENT_TYPE - CONTENT_LENGTH - REMOTE_ADDR - REMOTE_PORT - REMOTE_HOST 	<ul style="list-style-type: none"> - CGI program - Servlet service application

Directive that can be used	Environment variable that can be specified	Request that can be used
	<ul style="list-style-type: none"> - REMOTE_USER - REMOTE_IDENT - AUTH_TYPE - DOCUMENT_ROOT - SERVER_ADMIN - SERVER_NAME - SERVER_ADDR - SERVER_PORT - SERVER_SIGNATURE - SERVER_SOFTWARE 	
	<ul style="list-style-type: none"> - REQUEST_METHOD - REQUEST_URI - GATEWAY_INTERFACE - SCRIPT_NAME - SCRIPT_FILENAME - SERVER_PROTOCOL - PATH_INFO - PATH_TRANSLATED - QUERY_STRING 	<ul style="list-style-type: none"> - CGI program

Note 1) The module "mod_unique_id" must be set in the LoadModule directive.

Note 2) The [SSLNotifyVers](#) directive must be set to "On". Optional (default: On).

Note 3) The [SSLCertExpand](#) directive must be set to "On". Optional (default: On).

URL Rewrite

The URL is rewritten using the rewrite function according to the value set for the environment variable.

The directives that can be used by the environment variables, the environment variables that can be specified in those directives and the requests that can be used by those environment variables are shown below. For details on the environment variables, refer to "[List of Variables](#)".

Directive that can be used	Environment variable that can be specified	Request that can be used
<ul style="list-style-type: none"> - RewriteCond (test string"% {ENV:environment variable name}") - RewriteRule (conversion string"% {ENV:environment variable name}") 	<ul style="list-style-type: none"> - UNIQUE_ID (Note 1) - HTTPS z - HTTPS_CIPHER (Note 2) - HTTPS_SECRETKEYSIZE (Note 2) - TZ - SSL_CLIENT_CN (Note 2)(Note 3) 	<ul style="list-style-type: none"> - Static content - CGI program - Servlet service application

Directive that can be used	Environment variable that can be specified	Request that can be used
	<ul style="list-style-type: none"> - SSL_CLIENT_C (Note 2)(Note 3) - SSL_CLIENT_EMAIL (Note 2)(Note 3) - SSL_CLIENT_O (Note 2)(Note 3) - SSL_CLIENT_OU (Note 2)(Note 3) - SSL_CLIENT_T (Note 2)(Note 3) - SSL_CLIENT_PHONE (Note 2)(Note 3) - SSL_CLIENT_ST (Note 2)(Note 3) - SSL_CLIENT_L (Note 2)(Note 3) - Arbitrary environment variable 	

Note 1) The module "mod_unique_id" must be set in the LoadModule directive.

Note 2) The [SSLNotifyVers](#) directive must be set to "On". Optional (default: On).

Note 3) The [SSLCertExpand](#) directive must be set to "On". Optional (default: On).

Server Variable

The server variables are used as shown below.

URL Rewrite

The URL is rewritten using the rewrite function according to the value set for the server variable.

The directives that can be used by the server variables and the server variables that can be specified in those directives are shown below. For details on the server variables, refer to "[List of Variables](#)".

Directive that can be used	Server variable that can be specified
<ul style="list-style-type: none"> - RewriteCond (Test string "%{server variable}") - RewriteRule (Substitution string "%{server variable}") 	<ul style="list-style-type: none"> - HTTP_USER_AGENT - HTTP_REFERER - HTTP_COOKIE - HTTP_FORWARDED - HTTP_HOST - HTTP_PROXY_CONNECTION - HTTP_ACCEPT - REMOTE_ADDR - REMOTE_PORT - REMOTE_HOST - REMOTE_USER - REMOTE_IDENT

Directive that can be used	Server variable that can be specified
	<ul style="list-style-type: none"> - THE_REQUEST - REQUEST_METHOD - REQUEST_URI - SERVER_PROTOCOL - REQUEST_FILENAME - SCRIPT_FILENAME - PATH_INFO - QUERY_STRING - AUTH_TYPE - IS_SUBREQ - DOCUMENT_ROOT - SERVER_ADMIN - SERVER_NAME - SERVER_ADDR - SERVER_PORT - SERVER_SOFTWARE - API_VERSION - TIME_YEAR - TIME_MON - TIME_DAY - TIME_HOUR - TIME_MIN - TIME_SEC - TIME_WDAY - TIME

List of Variables

A list of environment variables and server variables is shown below.

	Variable	Content
HTTP header information	HTTP_USER_AGENT	User-Agent header content
	HTTP_REFERER	Referer header content
	HTTP_COOKIE	Cookie header content
	HTTP_FORWARDED	Forwarded header content
	HTTP_HOST	Host header content
	HTTP_PROXY_CONNECTION	Proxy-Connection header content
	HTTP_ACCEPT	Accept header content

	Variable	Content
	CONTENT_TYPE	Content-Type header content
	CONTENT_LENGTH	Content-Length header content
Connection/request information	REMOTE_ADDR	IP address of the client
	REMOTE_PORT	Port number of the client
	REMOTE_HOST	Host name of the client
	REMOTE_USER	User Name
	REMOTE_IDENT	User name identifier
	THE_REQUEST	HTTP request line
	REQUEST_METHOD	Request method
	REQUEST_URI	Request URI
	REQUEST_FILENAME	Full path of the contents file
	GATEWAY_INTERFACE	Version of CGI
	SCRIPT_NAME	File path of CGI program
	SCRIPT_FILENAME	SCRIPT_NAME converted to full path on the system
	SERVER_PROTOCOL	Protocol version
	PATH_INFO	Data passed in CGI program path format
	PATH_TRANSLATED	PATH_INFO converted to full path on the system
	QUERY_STRING	Query string
	AUTH_TYPE	Types of authentication
	UNIQUE_ID	Unique ID granted per request
	HTTPS	SSL communication type - on: HTTPS communication - off: HTTP communication
	HTTPS_CIPHER	Encryption format used for SSL communication
HTTPS_SECRETKEYSIZE	Key length used for SSL communication	
IS_SUBREQ	Subrequest information - true: The request being processed is a subrequest - false: The request being processed is not a subrequest	
Server internal information	DOCUMENT_ROOT	Value set for the DocumentRoot directive (Path of document route)
	SERVER_ADMIN	Value set for the ServerAdmin directive (Server Administrator e-mail address)
	SERVER_NAME	Value set for the ServerName directive (Host name of Server, or IP address and Port number)
	SERVER_ADDR	IP address of the web server
	SERVER_PORT	Port number of the web server
	SERVER_SIGNATURE	Server signature
	SERVER_SOFTWARE	Server version
	API_VERSION	Version of the web server program (A:I) - A: Major version

	Variable	Content
		- I: Minor version
System information	TZ	Time zone
	TIME_YEAR	Year (4 digit year): YYYY
	TIME_MON	Month (2 digit): MM
	TIME_DAY	Date (2 digit): DD
	TIME_HOUR	Hour (2 digit): hh
	TIME_MIN	Minute (2 digit): mm
	TIME_SEC	Second (2 digit): ss
	TIME_WDAY	Week (1 digit) - 0: Sunday - 1: Monday - 2: Tuesday - 3: Wednesday - 4: Thursday - 5: Friday - 6: Saturday
	TIME	Year Month Date Hour Minutes Seconds (14 digit): YYYYMMDDhhmmss
Client certificate information	SSL_CLIENT_CN	First and last name
	SSL_CLIENT_C	Country
	SSL_CLIENT_EMAIL	Mail address
	SSL_CLIENT_O	Organization name
	SSL_CLIENT_OU	Organizational unit name
	SSL_CLIENT_T	Title
	SSL_CLIENT_PHONE	Telephone number
	SSL_CLIENT_ST	State/Prefecture
	SSL_CLIENT_L	Street

Appendix C Setting the URL Rewrite

There are several ways of configuring the URL rewrite settings specified from the client (web browser), depending on the conversion type. Set the URL rewrite according to the web server operation method.

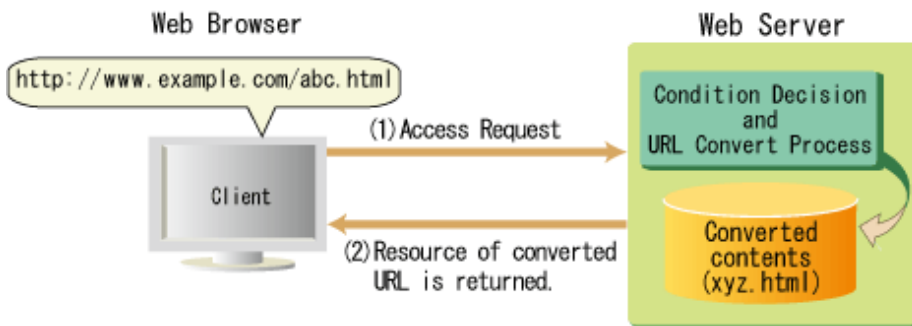
A functional overview of the conversion type, and the settings availability/settings method for that conversion type, are explained below.

- [Functional overview of the conversion type](#)
- [Settings availability/settings methods for the conversion type](#)

Functional overview of the conversion type

Internal Redirect

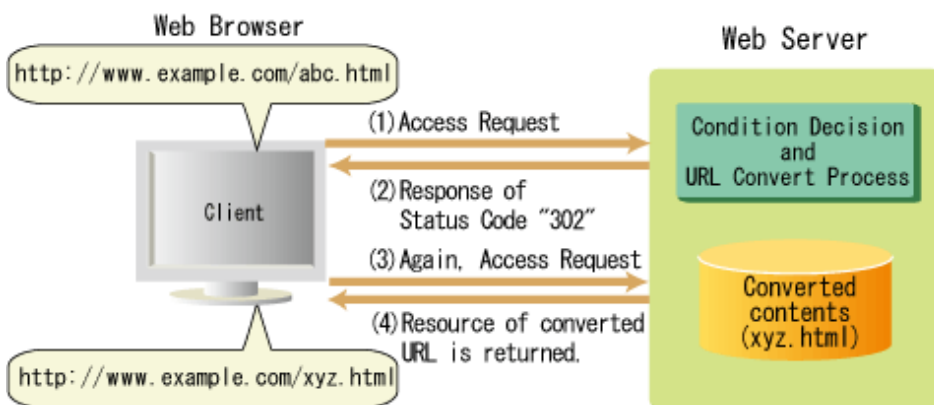
Internal redirect is used to rewrite the path in the URL. The internal redirect processing flow is shown below.



1. Specify a URL in the client, so that the client makes an access request to the web server.
2. The web server determines whether the request from the client has satisfied the URL rewrite conditions. If it has, it converts the URL and returns a response for the converted URL to the client.

External Redirect

External redirect is used to rewrite the URL to a new URL. The external redirect processing flow is shown below.



1. Specify a URL in the client, so that the client makes an access request to the web server.
2. The web server determines whether the request from the client has satisfied the URL rewrite conditions. If it has, it sets the converted URL in the Location header and returns a response containing status code "302" (Moved Temporarily).

Note

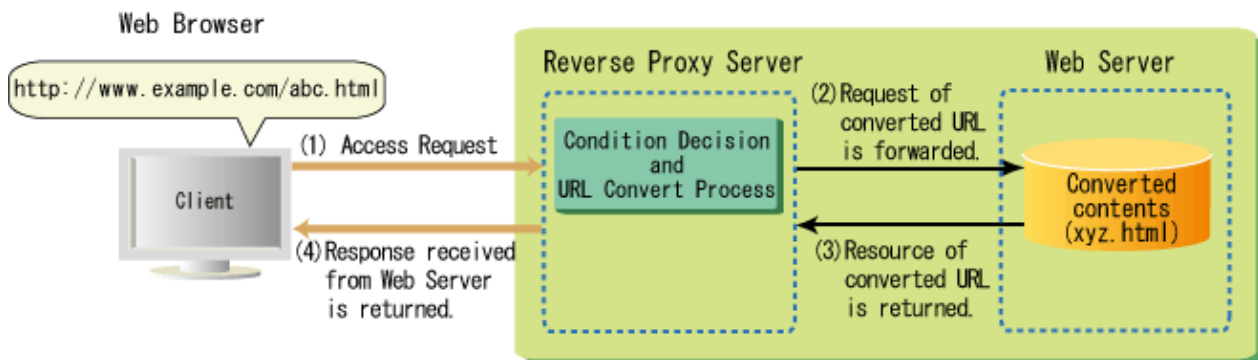
Depending on the settings, the response may contain status code "301" (Moved Permanently) or "303" (See Other).

3. Specify the URL that is set in the Location header in the client, so that the client again makes an access request to the web server.
4. The web server returns a response to the client for the request from the client.

Reverse Proxy

To process a request for which the URL is converted on the same web server without using redirect, run the reverse proxy server and the web server on a single web server.

The processing flow using the reverse proxy is shown below.

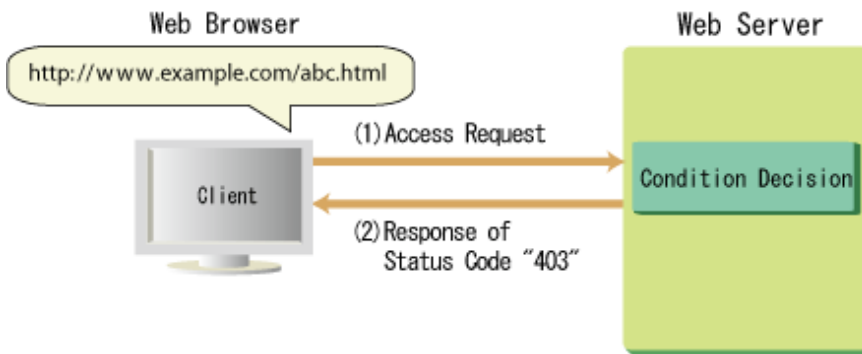


1. Specify a URL in the client, so that the client makes an access request to the reverse proxy server.
2. The reverse proxy server determines whether the request from the client has satisfied the URL rewrite conditions. If it has, it forwards the request for which the URL is converted to the web server.
3. The web server returns a response for the request for which the URL is converted to the reverse proxy server.
4. The reverse proxy server returns the response received from the web server to the client.

Access Denied

If the request from the client has satisfied the access denied conditions, the access is denied.

The access denied processing flow is shown below.



1. Specify a URL in the client, so that the client makes an access request to the web server.
2. The web server determines whether the request from the client has satisfied the access denied conditions. If it has, it returns a response containing status code "403" (Forbidden) and denies access.

Settings availability/settings methods for the conversion type

To configure the URL rewrite settings, check the settings availability for the conversion type in the table below. If the settings can be configured, refer to each settings method before editing the environment definition file (httpd.conf).

Conversion type	Request communication type	URL after conversion			Setting availability	Setting method
Internal redirect	SSL is not used	SSL is not used	Virtual directory	Path to static content	Can be set	Setting method 1
				Path to CGI program	Can be set	Setting method 2
				Path to Servlet service application	Cannot be set	-
		Rewrite function	Path to static content	Can be set	Setting method 3	
			Path to CGI program	Can be set	Setting method 4	
			Path to Servlet service application	Cannot be set Note) Alternative method available	Alternate method: Setting method 9	
		SSL is used			Cannot be set	-
	SSL is used	SSL is not used			Cannot be set Note) Alternative method available	Alternate method: Setting method 9
SSL is used			Virtual directory	Path to static content	Can be set	Setting method 1

Conversion type	Request communication type	URL after conversion			Setting availability	Setting method
				Path to CGI program	Can be set	Setting method 2
				Path to Servlet service application	Cannot be set	-
			Rewrite function	Path to static content	Can be set	Setting method 3
				Path to CGI program	Can be set	Setting method 4
				Path to Servlet service application	Cannot be set	-
External redirect	SSL is not used / SSL is used	SSL is not used	Redirect function	Path to static content	Can be set	Setting method 5
				Path to CGI program		
				Path to Servlet service application		
			Rewrite function	Path to static content	Can be set	Setting method 6
				Path to CGI program		
				Path to Servlet service application		
		SSL is used	Redirect function	Path to static content	Can be set	Setting method 7
				Path to CGI program		
				Path to Servlet service application		
Rewrite function	Path to static content	Can be set	Setting method 8			
	Path to CGI program					
	Path to Servlet service application					
Reverse proxy	SSL is not used / SSL is used	SSL is not used	Rewrite function	Path to static content	Can be set	Setting method 9
				Path to CGI program		
				Path to Servlet service application		
		SSL is used		Cannot be set	-	
Access denied	SSL is not used / SSL is used	SSL is not used / SSL is used			Can be set	Setting method 10

Setting Method 1

To internally redirect the specified virtual directory "URL path" and "URL pattern" to the "file path"/"directory path" to the static content, set the path using one of the following methods:

Alias URLPath FilePath DirectoryPath

AliasMatch URLPattern FilePath DirectoryPath
--

Setting Method 2

To internally redirect the specified virtual directory "URL path" and "URL pattern" to the "file path"/"directory path" to the CGI program, set the path using one of the following methods:

Windows32/64

```
LoadModule cgi_module "C:/Interstage/F3FMahs/modules/mod_cgi.so"
ScriptAlias URLPath FilePath|DirectoryPath
```

```
LoadModule cgi_module "C:/Interstage/F3FMahs/modules/mod_cgi.so"
ScriptAliasMatch URLPattern FilePath|DirectoryPath
```

Solaris32/64 Linux32/64

```
LoadModule cgid_module "/opt/FJSVahs/modules/mod_cgid.so"
ScriptAlias URLPath FilePath|DirectoryPath
```

```
LoadModule cgid_module "/opt/FJSVahs/modules/mod_cgid.so"
ScriptAliasMatch URLPattern FilePath|DirectoryPath
```



For details on the setting CGI program execution permissions, refer to "[3.28 CGI Program Execution Permissions Settings](#)".

Setting Method 3

To internally redirect a request that satisfies the specified "URL pattern" rewrite conditions to the path to static content, set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
RewriteEngine On
RewriteRule URLPattern PathBeginningWithSlash
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"
RewriteEngine On
RewriteRule URLPattern PathBeginningWithSlash
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithSlash
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithSlash
```



To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 4

To internally redirect a request that satisfies the specified "URL pattern" rewrite conditions to the path to CGI program, set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithSlash [PT]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithSlash [PT]
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithSlash [PT]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
```



```
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithSlash [PT]
```

Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 5

To externally redirect the specified "URL"/ and "URL pattern" to the path to the static content/Servlet service application/CGI program, set the path using one of the following methods:

```
Redirect URL PathBeginningWithhttp://
```

```
RedirectMatch URLPattern PathBeginningWithhttp://
```

Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 6

To externally redirect the specified "URL pattern" rewrite conditions to the path to the static content/Servlet service application/CGI program, set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttp:// [R]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"
RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttp:// [R]
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
RewriteEngine On
```

```
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithhttp:// [R]
```

Solaris32/64 **Linux32/64**

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithhttp:// [R]
```



Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 7

To externally redirect the specified "URL" and "URL pattern" to the path to the static content/Servlet service application/CGI program, set the path using one of the following methods:

```
Redirect URL PathBeginningWithhttps://
```

```
RedirectMatch URLPattern PathBeginningWithhttps://
```



Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 8

To externally redirect the specified "URL pattern" rewrite conditions to the path to the static content/Servlet service application/CGI program path, set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttps:// [R]
```

Solaris32/64 **Linux32/64**

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttps:// [R]
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithhttps:// [R]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern PathBeginningWithhttps:// [R]
```



Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to ["3.28 CGI Program Execution Permissions Settings"](#).
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 9

To treat a request that satisfies the specified "URL pattern" rewrite conditions as a proxy request, and convert it to the path to the static content/Servlet service application/CGI program and forward it to the web server, set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
LoadModule proxy_module "C:/Interstage/F3FMahs/modules/mod_proxy.so"
LoadModule proxy_http_module "C:/Interstage/F3FMahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttp:// [P]
```

Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"
LoadModule proxy_module "/opt/FJSVahs/modules/mod_proxy.so"
LoadModule proxy_http_module "/opt/FJSVahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteRule URLPattern PathBeginningWithhttp:// [P]
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"
LoadModule proxy_module "C:/Interstage/F3FMahs/modules/mod_proxy.so"
```

```
LoadModule proxy_http_module      "C:/Interstage/F3FMahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteCond   TestString ConditionPattern
RewriteRule   URLPattern PathBeginningWithhttp:// [P]
```

Solaris32/64 **Linux32/64**

```
LoadModule rewrite_module         "/opt/FJSVahs/modules/mod_rewrite.so"
LoadModule proxy_module          "/opt/FJSVahs/modules/mod_proxy.so"
LoadModule proxy_http_module     "/opt/FJSVahs/modules/mod_proxy_http.so"

RewriteEngine On
RewriteCond   TestString ConditionPattern
RewriteRule   URLPattern PathBeginningWithhttp:// [P]
```



Note

- To redirect to a path to a CGI program, the settings must also be configured to allow the execution of CGI programs. For details on the setting, refer to "[3.28 CGI Program Execution Permissions Settings](#)".
- To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Setting Method 10

To deny access to a request that satisfies the specified "URL pattern" rewrite conditions by returning a response containing status code "403" (Forbidden), set the path using one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule   URLPattern - [F]
```

Solaris32/64 **Linux32/64**

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteRule   URLPattern - [F]
```

To add a rewrite condition using the RewriteCond directive, use one of the following methods:

Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond   TestString ConditionPattern
RewriteRule   URLPattern - [F]
```

Solaris32/64 **Linux32/64**

```
LoadModule rewrite_module "/opt/FJSVahs/modules/mod_rewrite.so"

RewriteEngine On
RewriteCond TestString ConditionPattern
RewriteRule URLPattern - [F]
```

Note

To rewrite a request for the Servlet service application, set the above directive in the <Location> section.

Information

Relating Directives

- Alias
- AliasMatch
- <Location>
- Redirect
- RedirectMatch
- [RewriteCond](#)
- [RewriteEngine](#)
- [RewriteRule](#)
- ScriptAlias
- ScriptAliasMatch

C.1 Relating Directives

Items which explain the directive

The items which explain the directive are shown below.

Name

Directive name

Synopsis

Directive format

Description

Functional overview of the directive

Context

Directive-set location indicated with one of the following keywords:

Global context

Setting used for action of the entire web server.

Virtual host

Setting which is available in the <VirtualHost> section and used for action of the virtual host.

Directory

Setting which is available in the <Directory>, <Location>, and <Files> sections and used for action in response to a request for a specified directory, URL, or file.

Default value

Value assumed when the directive is omitted. If a directive indicated with "None" is omitted, the directive function is disabled.

Initial value

Initial directive value

Module

Name of the module that implements the directive function. A directive with no module name indication is included in the basic module.

Note

Notes on the use of the directive

Examples

Directive example (included only for a directive which requires a complex setting).

C.1.1 RewriteCond

Name

RewriteCond

Synopsis

RewriteCond TestString CondPattern [flag]

Description

Sets the condition that will rewrite the URL. This directive can be set multiple times before the [RewriteRule](#) directive. If the test string value has satisfied the condition specified for CondPattern, the [RewriteRule](#) directive setting that follows will apply.

- TestString

Specify the test string using the following variables:

- \$N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the [RewriteRule](#) directive, URLPattern immediately before.

- %N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the RewriteCond directive, CondPattern that satisfied the condition finally.

- %{server variable name}

Specify the server variable.

- %{ENV:environment variable name}

Specify the environment variable.

- %{HTTP:header name}

Specify a HTTP request header.

- CondPattern

Specify a regular expression for the condition that will determine the test string value. To negate the pattern, prefix it with an exclamation mark (!).

- flag (OPTIONAL)

Specify the flag that will control the condition decision. Separate multiple flags with a comma (,).

The valid values are described below:

- nocase (or, NC)

Specifies that case sensitivity is not be used.

- ornext (or, OR)

Specify this when multiple cases of this directive are specified for the OR condition. If this flag is not specified, then the AND condition will be used.

- novary (or, NV)

If a HTTP request header is specified in the TestString, this flag prevents this header from being added to the Vary header of the response.

Context

Global context, Virtual host, Directory

Default Value

None

Module

mod_rewrite

Note

- This directive will be enabled when the [RewriteEngine](#) directive is set to "On".
- Set this directive for each virtual host separately.

C.1.2 RewriteEngine

Name

RewriteEngine

Synopsis

RewriteEngine On|Off

Description

Enables/disables the rewrite feature, which enables flexible rewriting of the URL (note that the URL rewrite conditions and rules are set in the [RewriteCond](#) and [RewriteRule](#) directives).

The valid values are described below:

- On
- Off

Context

Global context, Virtual host, Directory

Default Value

```
RewriteEngine Off
```

Module

mod_rewrite

Note

Set this directive for each virtual host separately.

C.1.3 RewriteRule

Name

RewriteRule

Synopsis

RewriteRule URLPattern Substitution [flag]

Description

Sets the rule for rewriting the URL.

By combining this with a rewrite-related directive such as the [RewriteCond](#) directive, flexible rewriting of the URL is possible.

- URLPattern

Specify the rewrite target URL, using a regular expression.

If a URL-encoded URL is specified, the rewrite target URL is the decoded URL.

- Substitution

Specify the URL that will be rewritten if the URL pattern is matched:

- \$N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in URLPattern.

- %N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the [RewriteCond](#) directive, CondPattern that satisfied the condition finally.

- %{server variable name}

Specify the server variable.

- %{ENV:environment variable name}

Specify the environment variable.

- %{HTTP:header name}

Specify an optional HTTP request header.

- -

The URL is not rewritten.

- flag (OPTIONAL)

Specify the flag enclosed in square brackets ([]). Separate multiple flags with a comma (,).

The valid values are described below:

- redirect[=status] (or, R[=status])

Executes external redirect in the URL that was rewritten.

The valid status types are described below (if [=status] is omitted, it will be redirected using status code "302" (Moved Temporarily)):

- permanent (or, 301)

Redirected using status code "301" (Moved Permanently).

- temp (or, 302)

Redirected using status code "302" (Moved Temporarily).

- seeother (or, 303)

Redirected using status code "303" (See Other).

- forbidden (or, F)

Returns status code "403" (Forbidden). Specify this as the condition that was set for the [RewriteCond](#) directive to forbid access to the web server.

- gone (or, G)

Returns status code "410" (Gone). Specify this to notify the client of the fact that a page that does not exist was accessed.

- proxy (or, P)

If the rule is matched, the URL that was rewritten is assumed to be a proxy request and is used as a reverse proxy.

If this flag is specified, mod_proxy, mod_proxy_connect and mod_proxy_http module must be set for the LoadModule directive.

- last (or, L)

If the rule is matched, URL rewrite processing is completed. Rules that follow will not be applied.

- next (or, N)

Restarts a series of rewrite processing rules starting from the first rule. A URL that has already been rewritten will be a target. To specify this flag, specify the completion condition appropriately so that rewrite processing will not be executed infinitely.

- chain (or, C)

If the rule is matched, the rules that follow will be applied. If the rule is not matched, none of the rules that follow will be applied.

- type=MIME type (or, T=MIME type)

If the rule is matched, the specified MIME type will be set for the Content-TypeURL header.

Note

The MIME type specified is invalid if a Servlet service application is accessed and a MIME type has been set for that application.

- nosubreq (or, NS)

The rule will not be applied for subrequests that occur in the web server.

This is used when subrequests will occur for the file that was specified in the DirectoryIndex directive when the client specified a URL with a forward slash (/) at the end. However, the rule will not be applied for these subrequests.

- nocase (or, NC)

The rule will be applied without upper/lower case-sensitivity.

- qsappend (or, QSA)

If there is a query string (the string after the question mark (?) in the URL) in the URL before it is rewritten and Substitution, this appends an ampersand (&) and the query string that was specified in the URL before it was rewritten to the end of Substitution. If this flag is not specified, the query string will be overwritten by Substitution.

- noescape (or, NE)

URL escape at the time of the rewrite will be suppressed.

Normally, special characters such as the percentage sign (%) and semicolon (;) are escaped to a hexadecimal expression "%25" or "%3b". If this flag was specified, however, they will not be escaped.

- passthrough (or, PT)

Control will be passed to another module after the URL is rewritten.

Specify this when the Alias directive, ScriptAlias directive, and Redirect directive are used for the URL that was rewritten.

- skip=numeric (or, S=numeric)

If the rule is matched, application of the rules that follow will be skipped for the number of rules that was specified in the numeric.

- env=environment variable:value (or, E=environment variable:value)

If the rule is matched, the value for the environment variable that was specified will be set. \$N and %N can also be specified in the same way as Substitution for the value. For details on how to specify \$N and %N, refer to "Substitution" above.

Context

Global context, Virtual host, Directory

Default Value

None

Module

mod_rewrite

Note

- This directive will be enabled when the setting is for the rewrite feature to be used (when the [RewriteEngine](#) directive has been set to "On").
- To use this directive with a virtual host, set the directive for each virtual host separately. When this directive is set in the virtual host, the URL will be redirected internally if the host name of the URL that is to be rewritten and the address string that was specified in the <VirtualHost> section match. To redirect the URL externally, specify "redirect[=status] (or, R[=status])" in the flag setting.
- To specify a Servlet service application URL for Substitution, set external redirect or a reverse proxy. For details on how to set external redirect or the reverse proxy, refer to the [examples](#) below.

Examples

The URLs that are rewritten according to each rule that was set in this directive when a request is received from the client are shown in the table below.

Settings content	Request from the client	URL after replacement (Note)
RewriteRule ^/somepath(.*) /otherpath\$1	GET /somepath/pathinfo	/otherpath/pathinfo (internal redirect)
RewriteRule ^/somepath(.*) /otherpath\$1 [R]	GET /somepath/pathinfo	http://thishost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://thishost/otherpath\$1	GET /somepath/pathinfo	/otherpath/pathinfo (internal redirect)
RewriteRule ^/somepath(.*) http://thishost/otherpath\$1 [R]	GET /somepath/pathinfo	http://thishost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://otherhost/otherpath\$1	GET /somepath/pathinfo	http://otherhost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://originhost/otherpath\$1 [P]	GET /somepath/pathinfo	http://originhost/otherpath/pathinfo (reverse proxy)
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1 [PT]	GET /test.cgi?abc	/cgi-bin/test.cgi?abc
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1 [PT,QSA]	GET /test.cgi?abc	/cgi-bin/test.cgi?abc
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1?xyz [PT]	GET /test.cgi?abc	/cgi-bin/test.cgi?xyz
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1?xyz [PT,QSA]	GET /test.cgi?abc	/cgi-bin/test.cgi?xyz&abc

Note) The meaning of each host name is as follows:

- thishost: Web server in which the rules have been set
- otherhost: Other web server
- originhost: Content generation host web server when a proxy is used