

Bytix Archaea tools Command Reference

Index

1	Command reference.....	24
1.1	hcpd.....	24
1.1.1	f, foreground.....	25
1.1.2	V, version.....	25
1.1.3	h, help.....	25
1.1.4	t, config-test.....	26
1.1.5	system-info.....	29
1.1.6	run-host-benchmark.....	30
1.1.7	run-host-benchmark-categories.....	31
1.1.8	q, quit.....	31
1.1.9	c, config-file.....	32
1.1.10	l, log-file.....	32
1.1.11	L, stat-log-file.....	33
1.1.12	p, pid-file.....	33
1.1.13	k, license.....	34
1.1.14	auth-keys.....	35
1.1.15	auth-keys-uid.....	35
1.1.16	auth-keys-user.....	35
1.1.17	auth-keys-hcp-users.....	36
1.1.18	auth-keys-sys-auth-disabled.....	36
1.1.19	auth-keys-sys-auth-regardless-user-def.....	36
1.1.20	auth-keys-no-supp-groups.....	37
1.1.21	investigation.....	37
1.2	hcpd_winserv.....	37

Bytix Archaea tools Command Reference

1.2.1	version.....	38
1.2.2	configuration file.....	38
1.2.3	log file.....	38
1.2.4	statistics file.....	38
1.2.5	license.....	38
1.3	hcp.....	38
1.3.1	p, permission.....	42
1.3.2	R, recursive.....	43
1.3.3	Y, anydirs.....	43
1.3.4	g, regex.....	43
1.3.5	y, verify.....	44
1.3.6	z, compress.....	44
1.3.7	s, copy-linkfile.....	44
1.3.8	S, follow-linkdir.....	44
1.3.9	H, dereference-src.....	45
1.3.10	e, no-emptyfile.....	45
1.3.11	E, no-emptydir.....	45
1.3.12	d, no-dotfile.....	46
1.3.13	D, no-dotdir.....	46
1.3.14	I, copy-hidden.....	46
1.3.15	A, archive-check.....	46
1.3.16	sparse.....	47
1.3.17	q, quiet.....	47
1.3.18	r, resume.....	47
1.3.19	N, no-send.....	48

Bytix Archaea tools Command Reference

1.3.20	n, no-diskio.....	48
1.3.21	hpfp	49
1.3.22	wss.....	49
1.3.23	fio-extension.....	50
1.3.24	fio-direct.....	50
1.3.25	fio-async-linux	51
1.3.26	V, version	51
1.3.27	config-test.....	51
1.3.28	system-info.....	53
1.3.29	run-host-benchmark	54
1.3.30	run-host-benchmark-categories.....	55
1.3.31	h, help	55
1.3.32	m, copy-mode.....	56
1.3.33	o, overwrite.....	56
1.3.34	a, fail-action.....	57
1.3.35	user.....	57
1.3.36	password.....	58
1.3.37	f, source-file.....	58
1.3.38	source-file-host.....	59
1.3.39	port.....	60
1.3.40	config-file	60
1.3.41	config-option	61
1.3.42	show-config-options.....	61
1.3.43	hcp-diag.....	61
1.3.44	stat-log-file	62

Bytix Archaea tools Command Reference

1.3.45	hcp-out.....	62
1.3.46	multi-run.....	65
1.3.47	no-diskio-keep-read	66
1.3.48	no-diskio-keep-write.....	66
1.3.49	no-diskio-keep-memalign	66
1.3.50	no-skip-hcp-file	67
1.3.51	no-integrity-on-resume.....	67
1.3.52	no-agent.....	67
1.3.53	ident-select.....	68
1.3.54	overwrite-als-temp-file	68
1.3.55	preserve-win-read-only	68
1.3.56	udp.....	69
1.3.57	ws.....	70
1.3.58	wss-no-check-certificate.....	70
1.3.59	ws-proxy-direct.....	70
1.3.60	ws-proxy	71
1.3.61	hfp-cong.....	71
1.3.62	hfp-mss.....	71
1.3.63	hfp-sndbuf.....	72
1.3.64	hfp-rcvbuf	72
1.3.65	fio-direct-align	73
1.3.66	fio-direct-align-local	73
1.3.67	fio-direct-align-remote.....	73
1.3.68	fio-direct-malloc.....	74
1.3.69	fio-direct-reuse-aligned	75

Bytix Archaea tools Command Reference

1.3.70	fio-direct-align-threshold	75
1.3.71	fio-async-max-events	75
1.3.72	fio-async-max-get-events	76
1.3.73	fio-async-get-events-timeo	76
1.3.74	fio-fallocate	77
1.3.75	fio-fallocate-unit.....	77
1.3.76	fio-no-extension-local	78
1.3.77	fio-no-extension-remote.....	78
1.3.78	fio-extension-always	78
1.3.79	reading-dev	79
1.3.80	reading-dev-via-mmap.....	79
1.3.81	transfer-expire.....	79
1.3.82	no-out-of-order-header-messaging.....	79
1.3.83	mcd.....	79
1.3.84	auto-resume.....	80
1.3.85	include-conf-from-cwd.....	80
1.3.86	no-earlier-serv-compat	80
1.4	hsync	81
1.4.1	v, verbose	86
1.4.2	q, quiet.....	86
1.4.3	c, checksum	86
1.4.4	a, archive	87
1.4.5	r, recursive.....	87
1.4.6	R, relative	87
1.4.7	no-implied-dirs.....	87

Bytix Archaea tools Command Reference

1.4.8	b, backup	88
1.4.9	backup-dir	88
1.4.10	suffix	89
1.4.11	u, update.....	89
1.4.12	inplace.....	89
1.4.13	d, dirs.....	89
1.4.14	l, links	90
1.4.15	L, copy-links.....	90
1.4.16	copy-unsafe-links	91
1.4.17	safe-links	91
1.4.18	k, copy-dirlinks	92
1.4.19	K, keep-dirlinks	92
1.4.20	p, perms.....	92
1.4.21	E, executability.....	93
1.4.22	chmod.....	93
1.4.23	o, owner	94
1.4.24	g, group	94
1.4.25	devices	94
1.4.26	specials	95
1.4.27	D	95
1.4.28	t, times.....	95
1.4.29	O, omit-dir-times.....	95
1.4.30	J, omit-link-times	96
1.4.31	super.....	96
1.4.32	dry-run.....	96

Bytix Archaea tools Command Reference

1.4.33	auto-rerun	97
1.4.34	W, whole-file.....	97
1.4.35	one-file-system	97
1.4.36	existing.....	98
1.4.37	ignore-existing.....	98
1.4.38	del	98
1.4.39	delete	99
1.4.40	delete-before	99
1.4.41	delete-during.....	99
1.4.42	delete-delay	99
1.4.43	delete-after.....	100
1.4.44	delete-excluded	100
1.4.45	force	100
1.4.46	max-delete.....	101
1.4.47	max-size.....	101
1.4.48	min-size	102
1.4.49	partial	102
1.4.50	partial-dir.....	102
1.4.51	m, prune-empty-dirs	103
1.4.52	numeric-ids.....	103
1.4.53	usermap.....	104
1.4.54	groupmap.....	104
1.4.55	chown	105
1.4.56	l, ignore-times.....	105
1.4.57	size-only	105

Bytix Archaea tools Command Reference

1.4.58	@, modify-window.....	106
1.4.59	T, temp-dir.....	106
1.4.60	z, compress.....	107
1.4.61	compress-level.....	107
1.4.62	hcp-exclude	107
1.4.63	f, filter	108
1.4.64	exclude.....	109
1.4.65	exclude-from	109
1.4.66	include.....	110
1.4.67	include-from.....	111
1.4.68	files-from.....	111
1.4.69	stats.....	111
1.4.70	h, human-readable	112
1.4.71	progress.....	112
1.4.72	P.....	112
1.4.73	i, itemize-changes	113
1.4.74	out-format	113
1.4.75	log-file	114
1.4.76	bwlimit.....	114
1.4.77	stop-at.....	115
1.4.78	stop-after	115
1.4.79	V, version	116
1.4.80	config-test.....	116
1.4.81	h, help	119
1.5	hrm.....	119

Bytix Archaea tools Command Reference

1.5.1	f, force.....	121
1.5.2	R, recursive.....	121
1.5.3	d, dir	122
1.5.4	i	122
1.5.5	l	122
1.5.6	V, version.....	123
1.5.7	config-test	123
1.5.8	h, help	124
1.5.9	host.....	124
1.5.10	port.....	125
1.5.11	hcp-out.....	125
1.6	hcp-ls.....	126
1.6.1	q, query-cmdname.....	127
1.6.2	o, cmd-options.....	128
1.6.3	V, version.....	128
1.6.4	config-test	128
1.6.5	host.....	130
1.6.6	port.....	130
1.6.7	hcp-out.....	131
1.7	hmkdir	131
1.7.1	p, parents.....	133
1.7.2	V, version.....	133
1.7.3	config-test	133
1.7.4	h, help	135
1.7.5	host.....	135

Bytix Archaea tools Command Reference

1.7.6	port.....	135
1.7.7	hcp-out.....	136
1.8	hpwd	136
1.8.1	L, logical	138
1.8.2	P, physical	138
1.8.3	V, version.....	138
1.8.4	config-test	139
1.8.5	h, help	140
1.9	hmv	140
1.9.1	f, force.....	142
1.9.2	i, interactive	142
1.9.3	N, no-overwrite.....	142
1.9.4	V, version.....	143
1.9.5	config-test	143
1.9.6	h, help	144
1.9.7	host.....	145
1.9.8	port.....	145
1.9.9	hcp-out.....	145
1.10	hln	146
1.10.1	f, force.....	148
1.10.2	i, interactive	148
1.10.3	N, no-dereference	149
1.10.4	s, symbolic	149
1.10.5	L, logical.....	149
1.10.6	P, physical.....	149

Bytix Archaea tools Command Reference

1.10.7	symlink-target-expand-relative	150
1.10.8	symlink-target-accept-expand-relative	150
1.10.9	V, version	151
1.10.10	config-test.....	151
1.10.11	h, help	152
1.10.12	host.....	152
1.10.13	port.....	153
1.10.14	hcp-out.....	153
1.11	hchmod	154
1.11.1	R, recursive.....	156
1.11.2	V, version	156
1.11.3	config-test.....	156
1.11.4	h, help	157
1.11.5	host.....	158
1.11.6	port.....	158
1.11.7	hcp-out.....	158
1.12	hchown.....	159
1.12.1	d, no-dereference.....	161
1.12.2	R, recursive.....	161
1.12.3	s, follow-cmd-link-dir.....	161
1.12.4	S, follow-all.....	162
1.12.5	D, no-follow	162
1.12.6	V, version	162
1.12.7	config-test.....	163
1.12.8	h, help	164

Bytix Archaea tools Command Reference

1.12.9	host.....	164
1.12.10	port.....	165
1.12.11	hcp-out.....	165
2	Configuration reference.....	166
2.1	hcpd.conf.....	166
2.1.1	TCPListenAddress	170
2.1.2	TCPServiceSocketSendBuffer	171
2.1.3	HPFPListenAddress	172
2.1.4	UDPListenAddress.....	174
2.1.5	UDPServiceExtensionBufferSize	176
2.1.6	WSSListenAddress	176
2.1.7	WSSOptions.....	179
2.1.8	WSSCipherSuites.....	179
2.1.9	WSSCipherList.....	180
2.1.10	WSListenAddress.....	180
2.1.11	ListenServiceBonding	181
2.1.12	UseServerCertificateSecurity	182
2.1.13	RequireServerCertificateSecurity	183
2.1.14	ServerKeyFile	183
2.1.15	ServerCertificateFile.....	184
2.1.16	ServerCertificateChainFile	185
2.1.17	LocalPasswordAuthentication.....	185
2.1.18	PAMAuthentication.....	185
2.1.19	PubkeyAuthentication	186
2.1.20	WinLogonUserAuthentication.....	186

2.1.21	MaxAuthTries.....	187
2.1.22	PerformSystemAuthenticationRegardlessUsers.....	187
2.1.23	UserDirectoryFallbackAvailable.....	188
2.1.24	RejectOnUserHomeDirectoryNotFound.....	188
2.1.25	WinLogonUserNoRestrictedAccess.....	189
2.1.26	UsePrivilegeSeparation.....	189
2.1.27	PrivilegeSeparationMinimumUID.....	190
2.1.28	PrivilegeSeparationMinimumGID.....	190
2.1.29	PrivilegeSeparationUser.....	191
2.1.30	PrivilegeSeparationUmask.....	191
2.1.31	PrivilegeSeparationUmaskAnonymous.....	192
2.1.32	ApplyUserPermission.....	193
2.1.33	AllowUsers.....	193
2.1.34	AllowGroups.....	194
2.1.35	DenyUsers.....	195
2.1.36	DenyGroups.....	196
2.1.37	AuthorizedKeysSearchDir.....	197
2.1.38	AuthorizedKeysFile.....	197
2.1.39	AuthorizedKeysCommand.....	198
2.1.40	AuthorizedKeysCommandUser.....	198
2.1.41	CACertificateFile.....	199
2.1.42	CACertificatePath (reserved).....	199
2.1.43	CARevocationFile.....	200
2.1.44	CARevocationPath (reserved).....	200
2.1.45	OCSPRevocationEnabled.....	201

Bytix Archaea tools Command Reference

2.1.46	LocalUserFile	201
2.1.47	LocalPasswordFile	202
2.1.48	AcceptableCryptMethod	202
2.1.49	AcceptableDigestMethod	203
2.1.50	RequireDataIntegrityChecking	204
2.1.51	TransportCharEncoding	204
2.1.52	HostEncoding	205
2.1.53	HeaderCompress (reserved)	205
2.1.54	ContentCompress (reserved)	205
2.1.55	MaxConcurrentThread	205
2.1.56	MaxTotalConnection	206
2.1.57	MaxTcpConnection	206
2.1.58	MaxUdpConnection	206
2.1.59	MaxWsConnection	207
2.1.60	MaxConnectionPerUser	207
2.1.61	MaxConnectionPerSec	208
2.1.62	MaxReceiveFileSize	208
2.1.63	MaxSendFileSize	208
2.1.64	MaxRequestFileEntryAtOnce	209
2.1.65	MaxTotalBufferSize	209
2.1.66	MaxBufferSizePerConnection	209
2.1.67	MaxTotalReceiveRate	210
2.1.68	MaxTotalSendRate	210
2.1.69	MaxReceiveRate	211
2.1.70	MaxSendRate	211

Bytix Archaea tools Command Reference

2.1.71	MaxConnectionReceiveRate	211
2.1.72	MaxConnectionSendRate	212
2.1.73	InitHeaderBlockSize	212
2.1.74	InitContentBlockSize	213
2.1.75	MaxHeaderBlockSize	213
2.1.76	MaxContentBlockSize	214
2.1.77	FileLock	214
2.1.78	FileLockTrials	215
2.1.79	FileLockTrialInterval	215
2.1.80	AtomicLikeSaving	216
2.1.81	AtomicLikeSavingThreshold	217
2.1.82	AtomicLikeSavingRejectOverwriteRequest	217
2.1.83	TransportTimeout	217
2.1.84	IdleTimeout	218
2.1.85	DocPoint	218
2.1.86	DocPath	219
2.1.87	HomeIsolation	219
2.1.88	PermitAccessRead	219
2.1.89	PermitAccessWrite	220
2.1.90	PermitAccessOverwrite	220
2.1.91	PermitAccessDelete	221
2.1.92	PermitAccessRandomRead (reserved)	221
2.1.93	PermitAccessRandomWrite (reserved)	221
2.1.94	AccessList	222
2.1.95	Allow	222

Bytix Archaea tools Command Reference

2.1.96	Deny	223
2.1.97	SyslogOption.....	224
2.1.98	SyslogFacility.....	224
2.1.99	SystemLog	225
2.1.100	SystemLogLevel.....	227
2.1.101	ApplicationStatLog.....	228
2.1.102	TransportStatLog.....	229
2.1.103	SystemStatLog.....	230
2.1.104	FileOperationLog.....	232
2.1.105	CallbackScript	236
2.1.106	CallbackScriptHomeIsolation.....	239
2.1.107	CallbackScriptNoSymbolicLink.....	239
2.1.108	DisableMemoryManager.....	240
2.1.109	DiskBenchmarkPreAllocation.....	240
2.1.110	DiskBenchmarkPreAllocationSize	241
2.1.111	DiskBenchmarkDirectAlignmentSize	241
2.1.112	DiskBenchmarkAsyncNoWait (Reserved).....	242
2.1.113	DiskBenchmarkAsyncMaxEvents.....	242
2.1.114	DiskBenchmarkAsyncMaxGetEvents.....	242
2.1.115	DiskBenchmarkAsyncRequestPoolSize	243
2.1.116	DeepDiskBenchmarkFileSize	243
2.1.117	DeepDiskBenchmarkFreeSpaceRequired	243
2.1.118	DeepDiskBenchmarkBlockSizes	244
2.1.119	MemoryTransferConcurrency	244
2.1.120	MaxReadRate.....	245

2.1.121	MaxWriteRate	246
2.1.122	EnsureDestinationInFileTransfer	246
2.1.123	StatLogPerUserInPrivilegeSeparation	247
2.1.124	NoSupplementalGroupInPrivilegeSeparation.....	247
2.1.125	ApplicationStatLogSecurityEx	247
2.1.126	GetGrRMaxBufferSize	248
2.1.127	GetPwRMaxBufferSize	248
2.2	Client common command configuration list	249
2.2.1	RequireServerCertificateSecurity.....	251
2.2.2	RejectFallbackServerCertificateSecurity	252
2.2.3	IgnoreCertificateCNInvalid	252
2.2.4	IgnoreCertificateDateInvalid	252
2.2.5	IgnoreUnknownCA	253
2.2.6	IgnoreRevocation.....	253
2.2.7	WSSIgnoreCertificateCNInvalid	253
2.2.8	WSSIgnoreCertificateDateInvalid.....	254
2.2.9	WSSIgnoreUnknownCA.....	254
2.2.10	WSSIgnoreRevocation (reserved).....	255
2.2.11	WSSOptions.....	255
2.2.12	WSSCipherSuites.....	255
2.2.13	WSSCipherList	256
2.2.14	CACertificateFile	256
2.2.15	CACertificatePath (reserved)	257
2.2.16	CARevocationFile.....	257
2.2.17	CARevocationPath (reserved)	258

Bytix Archaea tools Command Reference

2.2.18	WSSCACertificateFile	258
2.2.19	OCSPRevocationEnabled	259
2.2.20	StrictHostKeyChecking.....	259
2.2.21	LocalPasswordAuthentication.....	259
2.2.22	PAMAuthentication.....	260
2.2.23	PubkeyAuthentication	260
2.2.24	WinLogonUserAuthentication.....	261
2.2.25	NumberOfPasswordPrompts.....	261
2.2.26	IdentitySearchDir	261
2.2.27	IdentityFile.....	263
2.2.28	AcceptableCryptMethod	264
2.2.29	AcceptableDigestMethod.....	265
2.2.30	DisableDataIntegrityChecking.....	266
2.2.31	AcceptDataIntegrityCheckingOnRejection	266
2.2.32	TransportCharEncoding	267
2.2.33	HostEncoding.....	267
2.2.34	CompressLevel	268
2.2.35	HeaderCompress.....	268
2.2.36	ContentCompress	269
2.2.37	MaxConcurrentThread	269
2.2.38	MaxReceiveFileSize.....	269
2.2.39	MaxSendFileSize	270
2.2.40	MaxRequestFileEntryAtOnce.....	270
2.2.41	MaxBufferSize	270
2.2.42	MaxReceiveRate.....	271

Bytix Archaea tools Command Reference

2.2.43	MaxSendRate	271
2.2.44	MaxConnectionReceiveRate	271
2.2.45	MaxConnectionSendRate	272
2.2.46	InitHeaderBlockSize	272
2.2.47	InitContentBlockSize	273
2.2.48	MaxHeaderBlockSize	273
2.2.49	MaxContentBlockSize	273
2.2.50	FileLock	274
2.2.51	FileLockTrials	274
2.2.52	FileLockTrialInterval	274
2.2.53	TransportTimeout	274
2.2.54	DiagnosticLog	274
2.2.55	DiagnosticLogLevel	276
2.2.56	ApplicationStatLog	276
2.2.57	TransportStatLog	277
2.2.58	UDPTransportExtensionBufferSize	278
2.2.59	TCPTransportSocketSendBuffer	279
2.2.60	PubkeyAuthenticationPrior	279
2.2.61	ApplicationStatLogSecurityEx	280
2.2.62	DiskBenchmarkPreAllocation	280
2.2.63	DiskBenchmarkPreAllocationSize	281
2.2.64	DiskBenchmarkDirectAlignmentSize	281
2.2.65	DiskBenchmarkAsyncNoWait (Reserved)	282
2.2.66	DiskBenchmarkAsyncMaxEvents	282
2.2.67	DiskBenchmarkAsyncMaxGetEvents	282

Bytix Archaea tools Command Reference

2.2.68	DiskBenchmarkAsyncRequestPoolSize	283
2.2.69	DeepDiskBenchmarkFileSize	283
2.2.70	DeepDiskBenchmarkFreeSpaceRequired	283
2.2.71	DeepDiskBenchmarkBlockSizes	284
2.3	hcp.conf	284
2.3.1	Include	285
2.3.2	UseProperCopyAndSync	285
2.3.3	AtomicLikeSaving	286
2.3.4	AtomicLikeSavingThreshold	286
2.3.5	AutoResumeTrials	287
2.3.6	AutoResumeTrialInterval	287
2.3.7	MemoryTransferConcurrency	287
2.3.8	MaxReadRate	288
2.3.9	MaxWriteRate	289
2.4	hsync.conf	289
2.4.1	Include	289
2.4.2	AutoRerunTrials	289
2.4.3	AutoRerunTrialInterval	290
2.5	hrm.conf	290
2.5.1	Include	290
2.6	hcp-ls.conf	290
2.6.1	Include	290
2.7	hmkdir.conf	290
2.7.1	Include	291
2.8	hpwd.conf	291

Bytix Archaea tools Command Reference

2.8.1	Include.....	291
2.9	hmv.conf	291
2.9.1	Include.....	291
2.10	hln.conf.....	291
2.10.1	Include	291
2.11	hchmod.conf.....	291
2.11.1	Include	291
2.12	hchown.conf.....	291
2.12.1	Include	291
2.13	users.....	292
2.14	passwd.....	293
3	Statistics reference	294
3.1	Application statistics.....	294
3.2	Transport statistics	298
3.2.1	TCP statistics	298
3.2.2	HpFP statistics	300
3.2.3	WS/WSS statistics	302
3.3	System statistics	303
4	Error code reference.....	305
4.1	Command end status	305
4.2	Configuration file error codes	306
4.3	File processing code.....	308
4.4	Signal control	311
4.5	Application signals.....	312
5	Command execution mode	313

Bytix Archaea tools Command Reference

5.1	Single running mode	314
5.2	Multiple running mode	315
6	Server backward compatibility conditions	317
7	Bytix Archaea tools restriction lists	318
8	Notation	318
9	revision history	319

1 Command reference

1.1 hcpd

Usage: hcpd [OPTION]...

or : hcpd -q [OPTION]...

or : hcpd --auth-keys [OPTION]... [PATH]

The hcpd daemon is the software which receives the instruction commands sent from the remote clients such as, the hcp (file transfer) command and the hrm (file delete) command and waits to execute them at the server side, which is available on Linux.

abbreviation	option	outline
f	foreground	foreground execution
V	version	version
h	help	help
t	config-test	loaded outcome of input parameter and configuration file
	system-info	show system info
	run-host-benchmark	run host benchmark
	run-host-benchmark-categories	specify measurement categories on the benchmark
q	quit	the stop command
c	config-file	configuration file
l	log-file	log file
L	stat-log-file	statistics log file
p	pid-file	PID file
k	license	license key file
	auth-keys	fetch authorized_keys
	auth-keys-uid	specify UID on fetching it
	auth-keys-user	specify user name on fetching it
	auth-keys-hcp-users	specify user definition file path on fetching it
	auth-keys-sys-auth-disabled	specify ability of system auth (PAM) on fetching it
	auth-keys-sys-auth-regardless-user-def	specify system auth (PAM) included always on fetching it
	auth-keys-no-supp-groups	disable supplemental groups on fetching

		it
	investigation	investigation mode

1.1.1 f, foreground

```
=====
Supported OS : Linux.x86
Format : -f | --foreground
=====
```

Start the hcpd daemon in the foreground mode.

```
--
Example :
[root@localhost ~]# hcpd -f ...
--
```

1.1.2 V, version

```
=====
Supported OS : Linux.x86
Format : -V | --version
=====
```

Display the hcpd daemon version.

```
--
Example :
[root@localhost ~]# hcpd -V
hcp server (hcpd) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS 4.
2.0-2)
--
```

1.1.3 h, help

```
=====
Supported OS : Linux.x86
Format : -h | --help
=====
```

Display the hcpd daemon help.

```
--
Example :
[root@localhost ~]# hcpd -h
--
```

1.1.4 t, config-test

```
=====
Supported OS : Linux.x86
Format : -t | --config-test
=====
```

Output the input parameters and the configuration data of the hcpd daemon.

```
--
Example :
[root@localhost ~]# hcpd -t
...

-- [Command Options] -----
---
Command parameters
foreground : disable
version    : disable
help       : disable
quit       : disable
config-test : enable
pid-file   : - [/var/run/hcpd.pid]
license    : - [/etc/hcp/license.key]
config-file : - [/etc/hcp/hcpd.conf]
log-file    : - [/var/log/hcpd.log]
stat-log-file : - [/var/tmp/.hcp.statistics]
run-host-benchmark : disable
run-host-benchmark-categories : - [all]
-- [Configuration Parameters] -----
---
Configuration parameters
PubkeyAuthentication      : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : no
MaxAuthTries              : 6
PerformSystemAuthenticationRegardlessUsers : no
```

Bytix Archaea tools Command Reference

```
UserDirectoryFallbackAvailable      : no
RejectOnUserHomeDirectoryNotFound  : no
UsePrivilegeSeparation              : yes [supp_group=yes]
PrivilegeSeparationMinimumUID       : 0
PrivilegeSeparationMinimumGID       : 0
PrivilegeSeparationUser              : nobody
PrivilegeSeparationUmask             : 0022 -
PrivilegeSeparationUmaskAnonymous  : 0002 -
ApplyUserPermission                  : yes
AllowUsers                           : -
AllowGroups                          : -
DenyUsers                           : -
DenyGroups                          : -
UseServerCertificateSecurity         : yes
RequireServerCertificateSecurity     : yes
HeaderCompress                       : yes
ContentCompress                      : yes
OCSPRevocationEnabled               : yes
AuthorizedKeysSearchDir              : -
AuthorizedKeysFile                   : - [ ~/.ssh/authorized_keys ~/.hcp/auth
orized_keys ]
AuthorizedKeysCommand                : -
LocalUserFile                       : - [/etc/hcp/users usage=overwrite]
LocalPasswordFile                   : - [/etc/hcp/passwd]
ServerKeyFile                       : - [/etc/hcp/key/server.key]
ServerCertificateFile               : - [/etc/hcp/cert/server.crt]
ServerCertificateChainFile           : - [/etc/hcp/cert/chain.crt]
CACertificateFile                   : - [/etc/hcp/cacert.pem]
CACertificatePath                   : - [/etc/ssl]
CARevocationFile                    : - [/etc/hcp/crl.pem]
CARevocationPath                    : - [/etc/ssl]
ProtocolVersion                     : 2
MaxConcurrentThread                  : 0
MaxTotalConnection                  : 150
MaxTcpConnection                    : 50
MaxUdpConnection                    : 50
MaxWsConnection                     : 50
MaxConnectionPerUser                : 50
MaxConnectionPerSec                  : 50
MaxRequestFileEntryAtOnce           : 50
MaxReceiveFileSize                  : unlimited
MaxSendFileSize                     : unlimited
MaxTotalBufferSize                  : 4294967296
MaxBufferSizePerConnection          : 104857600
MaxTotalReceiveRate                  : 100000000000
MaxTotalSendRate                    : 100000000000
MaxReceiveRate                      : 100000000000
```

Bytix Archaea tools Command Reference

```

MaxSendRate                : 1000000000000
MaxConnectionReceiveRate   : 1000000000000
MaxConnectionSendRate      : 1000000000000
InitHeaderBlockSize        : 51200
InitContentBlockSize       : 1048576
MaxHeaderBlockSize         : 51200
MaxContentBlockSize        : 1048576
TransportTimeout           : 180 sec
IdleTimeout                : 0 sec
FileLock                   : no
FileLockTrials              : 0
FileLockTrialInterval      : 3 sec
AtomicLikeSaving           : no .tmp NONE [threshold=0, reject_ow_
req=yes]
TCPListenAddress           : 0.0.0.0:874[TCP tcp1, mcd=1]
HPFPListenAddress          : 0.0.0.0:65520[HpFP udp1, sndbuf=10485
7600, rcvbuf=209715200, mss=-1, mcd=1]
ListenServiceBonding       : -
UDPServiceExtensionBufferSize : 2147483648
TCPServiceSocketSendBuffer : 0
AcceptableCryptMethod      : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod     : XXH3 SHA256 SHA160
RequireDataIntegrityChecking : yes
TransportCharEncoding      : UTF8
DocPoint                   : /home
  DocPath = /home
  HomeIsolation = no
  PermitAccessRead = yes
  PermitAccessWrite = yes
  PermitAccessOverwrite = yes
  PermitAccessDelete = yes
  PermitAccessRandomRead = no
  PermitAccessRandomWrite = no
DocPointEnd
HostEncoding               : UTF8
SyslogOption               : LOG_CONS | LOG_PID
SyslogFacility             : LOG_DAEMON
SystemLog                  : INFO yes Rotation[size=no:0:0, patter
n=no:] -[/var/log/hcpd.log]
ApplicationStatLog         : yes Rotation[size=no:0:0, pattern=n
o:]
TransportStatLog           : no Rotation[size=no:0:0, pattern=no:]
SystemStatLog              : yes Rotation[size=no:0:0, pattern=n
o:]
FileOperationLog           : no -[/var/log/hcpd.file.operation.lo
g] Rotation[size=no:0:0, pattern=no:]

```

```

    CallbackScript                : no Script[~/.hcp/callback.sh, data=~/.
hcp/callback]
    CallbackScriptHomeIsolation   : no [logical=no]
    CallbackScriptNoSymbolicLink  : no
    DisableMemoryManager          : yes
    EnsureDestinationInFileTransfer : yes
    StatLogPerUserInPrivilegeSeparation : no
    ApplicationStatLogSecurityEx   : yes
    MemoryTransferConcurrency      : 1 (wait_type cond, exp_nsec 1)
    MaxReadRate                   : unlimited
    MaxWriteRate                  : unlimited
    DiskBenchmarkPreAllocation     : none
    DiskBenchmarkPreAllocationSize : 0
    DiskBenchmarkDirectAlignmentSize : 0
    DiskBenchmarkDirectMalloc      : posix
    DiskBenchmarkAsyncNowait       : no
    DiskBenchmarkAsyncMaxEvents    : 16
    DiskBenchmarkAsyncMaxGetEvents : 1
    DiskBenchmarkAsyncGetEventsTimeout : 0 usec
    DiskBenchmarkAsyncRequestPoolSize : 32
    DeepDiskBenchmarkFileSize      : 17179869184
    DeepDiskBenchmarkFreeSpaceRequired : 34359738368
    DeepDiskBenchmarkBlockSizes    : 16KB 32KB 64KB 256KB 512KB 1MB 2MB 4M
B 8MB 16MB 24MB 32MB
    GetGrRMaxBufferSize           : 524288
    GetPwRMaxBufferSize           : 65536
-----
---
--

```

1.1.5 system-info

```

=====
Supported OS : Linux.x86
Format : --system-info
=====

```

This option tells hcpd to show the system information. The following contents will be displayed.

- CPU brand name
- Number of physical processors and logical processors
- Hardware acceleration information around AES function
- System memory size
- Kernel information (Linux)

- OS information
- Host name

When specifying this option twice, the following contents will be displayed.

- Disk consumption (df output, Linux)
- Network interface detail

--

Example :

```
[root@localhost ~]# hcpd --system-info ...
```

--

1.1.6 run-host-benchmark

Supported OS : Linux.x86

Format : --run-host-benchmark

This option tells hcpd to make a benchmark of the local host about the following performances.

- Security communication performance (AES, GCM/CTR/CBC mode, MD5, SHA1, SHA256)
- File integrity validation performance (XXH3, Parity)
- Disk reading & writing performance (Cached, Direct I/O)
- Memory copy performance

When this option is specified twice, the benchmark run with some additional conditions.

- Security communication performance (some additional AES benchmarks around block size and concurrency)
- File integrity validation performance (some additional benchmarks about Parity calculation)
- Disk reading & writing performance (some additional benchmarks around block size)
- Memory copy performance (an additional benchmark on concurrency)

--

Example :

```
[root@localhost ~]# hcpd --run-host-benchmark ...
```

--

1.1.7 run-host-benchmark-categories

```
=====
Supported OS : Linux.x86
Format : --run-host-benchmark-categories=<categories>
-----
categories
Default : all
Range of Values : secure, integrity, disk, memory, all
=====
```

You can specify measurement categories over which hcpd make the benchmark. The following values are available.

- secure (security communication performance)
- integrity (file integrity validation performance)
- disk (disk reading & writing performance)
- memory (memory copy performance)
- all (all of the values above)

Please use this option to reduce measurements when it takes a long time.

```
--
Example :
[root@localhost ~]# hcpd --run-host-benchmark-categories=disk,memory ...
--
```

1.1.8 q, quit

```
=====
Supported OS : Linux.x86
Format : -q | --quit
=====
```

hcpd newly to run sends the signal to terminate the hcpd daemon working.

It gets the process ID from the specified file in the pid-file option or the default file and send the signal with the process ID to terminate the hcpd working.

```
--
Example :
[root@localhost ~]# hcpd -q ...
--
```

1.1.9 c, config-file

```
=====
Supported OS : Linux.x86
Format : -c <config-file-path> | --config-file=<config-file-path>
-----

config-file-path
Default : none
Range of Values : path string of file system
=====
```

This option specifies the path of the configuration file that the hcpd daemon read.

```
--
Example :
[root@localhost ~]# hcpd -c /etc/hcp/hcpd2.conf ...
--
```

If this option is not specified, the configuration from the following file will be read.

/etc/hcp/hcpd.conf

1.1.10 l, log-file

```
=====
Supported OS : Linux.x86
Format : -l <log-file-path> | --log-file=<log-file-path>
-----

log-file-path
Default : none
Range of Values : path string of file system
=====
```

This option specifies a path of a file to which the hcpd daemon output logs.

```
--
Example :
[root@localhost ~]# hcpd -l /var/log/hcpd.log ...
--
```

When this option is not specified, the log is output as the standard output.

1.1.11 L, stat-log-file

```
=====
Supported OS : Linux.x86
Format : -L <log-file-path> | --stat-log-file=<log-file-path>
-----
log-file-path
Default : none
Range of Values : path string of file system
=====
```

This option specifies the path of the statistic log file which the hcpd daemon outputs.

--

Example :

```
[root@localhost ~]# hcpd -L /var/tmp/.hcp.statistics2 ...
```

--

Each statistics log is output in the specified path with suffix.

```
<spciified path>.system (system statistics)
<spciified path>.application (application statistics)
<spciified path>.transport.tcp.service_<service number>.<service port>.th
read_<thread number>.transport.tcp (TCPtransport statistics)
<spciified path>.transport.hpfp.service_<service number>.<t;service port>.
thread_<thread number>(HpFPtransport statistics)
<spciified path>.transport.ws.service_<service number>.<t;service port>.t
hread_<thread number>(WS/WSStransport statistics)
```

When it is output by a non-privileged user with StatLogPerUserInPrivilegeSeparation enabled, it is recorded in the following path.

```
<spciified path>.application.<UID>_<GID> (Linux)
<spciified path>.application.<Username> (Windows)
```

When this option is not specified, it is output in the following path.

```
/var/tmp/.hcp.statistics
```

1.1.12 p, pid-file

```
=====
Supported OS : Linux.x86
Format : -p <pid-file-path> | --pid-file=<pid-file-path>
-----
pid-file-path
Default : /var/run/hcpd.pid
```

Range of Values : path string of file system

=====

This option specifies the file path in order to output the process ID of the hcpd daemon process.

--

Example :

```
[root@localhost ~]# hcpd -p /var/run/hcpd2.pid ...
```

--

Please note that if plural daemon processes are going to run or another daemon process has already run, the same file path is unavailable.

1.1.13 k, license

=====

Supported OS : Linux.x86

Format : -k <license-key-path> | --license=<license-key-path>

license-key-path

Default : /etc/hcp/license.key

Range of Values : path string of file system

=====

The license key path is set.

--

Example :

```
[root@localhost ~]# hcpd -k /etc/hcp/license2.key ...
```

--

The path of the license key is specified. When this option is not specified, the license key will be read from the following path.

/etc/hcp/license.key

When the license key is not available to read, the trial license is applied with the following conditions.

total max throughput 1Gbps

Max throughput 1Gbps

TCP Max session 3

HpFP Max session 3

WS/WSS Max session 3

Max multiple connection degree per session 1

1.1.14 auth-keys

```
=====
Supported OS : Linux.x86
Format : --auth-keys
=====
```

This option tells hcpd to fetch public key data from the following files saved at a user home directory. The data will be written to the standard output.

- ~/.ssh/authorized_keys
- ~/.hcp/authorized_keys

When using this option, hcpd dose run as a service daemon.

When passing a path for this option, it will fetch the data form the given path where public keys are supposed to be saved at that place.

This option is primarily defined for hcpd fetching public keys on its public key authentication. Normally you do not have to use this option except for investigation of that fetching function (out of support on normal uses).

```
--
Example :
[root@localhost ~]# hcpd --auth-keys ... "~/.hcp/authorized_keys" // fetc
h only from the .hcp directory. suppress tilde expansion
--
```

1.1.15 auth-keys-uid

```
=====
Supported OS : Linux.x86
Format : --auth-keys-uid=<uid>
-----
uid
Default : none
Range of Values : UID number
=====
```

This option specifies a UID used on fetching public key data.

```
--
Example :
[root@localhost ~]# hcpd --auth-keys --auth-keys-uid=1000 ...
--
```

1.1.16 auth-keys-user

```
=====
Supported OS : Linux.x86
Format : --auth-keys-user=<user_name>
```

```
-----  
user_name  
Default : none  
Range of Values : Unix account user name  
=====
```

This option specifies a user name used on fetching public key data.

```
--  
Example :  
[root@localhost ~]# hcpd --auth-keys --auth-keys-uid=user01 ...  
--
```

1.1.17 auth-keys-hcp-users

```
=====  
Supported OS : Linux.x86  
Format : --auth-keys-hcp-users=<user_def_file_path>  
-----  
user_def_file_path  
Default : /etc/hcp/users  
Range of Values : path string on file system of user definition file  
=====
```

This option specifies a path string on a file system of user definition file.

```
--  
Example :  
[root@localhost ~]# hcpd --auth-keys --auth-keys-hcp-users=/etc/hcp/users.  
another.def ...  
--
```

1.1.18 auth-keys-sys-auth-disabled

```
=====  
Supported OS : Linux.x86  
Format : --auth-keys-sys-auth-disabled  
=====
```

This option tells hcpd to run fetching public key data as the system authentication (PAM) is disabled.

```
--  
Example :  
[root@localhost ~]# hcpd --auth-keys --auth-keys-sys-auth-disabled ...  
--
```

1.1.19 auth-keys-sys-auth-regardless-user-def

```
=====  
Supported OS : Linux.x86
```

Format : --auth-keys-sys-auth-regardless-user-def

=====

This option tells hcpd to run fetching public key data as the system authentication (PAM) will be performed regardless user definition.

--

Example :

```
[root@localhost ~]# hcpd --auth-keys --auth-keys-sys-auth-regardless-user-def ...
```

--

1.1.20 auth-keys-no-supp-groups

=====

Supported OS : Linux.x86

Format : --auth-keys-no-supp-groups

=====

This options disable supplemental groups on fetching public key data.

--

Example :

```
[root@localhost ~]# hcpd --auth-keys --auth-keys-no-supp-groups ...
```

--

1.1.21 investigation

=====

Supported OS : Linux.x86

Format : --investigation

=====

The hcpd daemon starts in the investigation mode. In the case of unexpected behaviors and so on, detailed log is output for the investigation. This mode is not suitable for the long-time use and the case where the high performance is required on the transmission, because a lot of logs are output. Kindly send the log to the application developer for its investigation, because it is not for users but for the developers.

1.2 hcpd_winserv

hcpd_winserv is a software that accepts the hcp (file transfer) and the hrm (file deletion) command instructions from the remote (client) and waits on the server side to execute the processing. It is provided as a service program in the Windows version but can't be executed on the command prompt .

1.2.1 version

The version of hcpd_winserv is recorded in the log file described below on starting the service.

--

Example :

```
hcp server (hcpd) 1.5.13_2 / Windows (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS
4.2.0-2)
```

--

1.2.2 configuration file

hcpd_winserv configuration is read from the following file.

C:/ProgramData/Clealink/HCP Tools/hcpd.conf

1.2.3 log file

The application log is written in the following file.

C:/ProgramData/Clealink/HCP Tools/hcpd.log

1.2.4 statistics file

The statistics log is output in the following path in the Windows version. In terms of the additional suffix, the same string is used as the one in the Linux version.

C:/ProgramData/Clealink/HCP Tools/Temp/_hcp.statistics

1.2.5 license

The license key is read from the following path.

C:/ProgramData/Clealink/HCP Tools/license.key

When the license key cannot be read, the same trial license as the one in the Linux version is supposed to be applied.

1.3 hcp

```
Local  : hcp [OPTION]... SOURCE [SOURCE]... DEST
or     : hcp [OPTION]... -f SOURCE_LIST_FILE DEST
```

Remote :

```
Push  : hcp [OPTION]... SOURCE [SOURCE]... [USER@]HOST[:PORT]:DEST
Pull  : hcp [OPTION]... [USER@]HOST[:PORT]:SOURCE [:SOURCE]... DEST
```

Remote using source file list :

```
Push  : hcp [OPTION]... -f SOURCE_LIST_FILE [USER@]HOST[:PORT]:DEST
```

Bytix Archaea tools Command Reference

```
Pull : hcp [OPTION]... -f SOURCE_LIST_FILE DEST
Pull : hcp [OPTION]... --source-file-host=HOST [--port=PORT] [--user=USER] -f SOURCE_LIST_FILE DEST
```

The hcp command works to transfer files between the remote server and the hcpd daemon and also to copy files in the local network.

abbreviation	option	outline
p	permission	keep source permission
R	recursive	recursive copy
Y	anydirs	search all directories (remove wildcard from regular expression.)
g	regex	file names recognized as regular expressions (but not in wildcard manner)
y	verify	verify data in the digest way
z	compress	compress
s	copy-linkfile	resolve the symbolic link (Dereference) and copy files
S	follow-linkdir	resolve the symbolic directory and copy files
H	dereference-src	resolve symbolic links specified on SOURCE to copy
e	no-emptyfile	skip copying empty files
E	no-emptydir	skip copying empty directories
d	no-dotfile	skip copying the files whose names start with '.'.
D	no-dotdir	skip copying the directories whose names start with '.'.
I	copy-hidden	copy the files with hidden attribute
A	archive-check	Copy the files with archive attribute
	sparse	Copy the files being aware of sparse files
q	quiet	suppress non-error messages
r	resume	Resume (the previous execution record is necessary)
N	no-send	no send on a transport but measure the disk I/O performance
n	no-diskio	measure the network I/O performance of communication protocol without disk I/O

Bytix Archaea tools Command Reference

		operations.
	hpfp	use the HpFP protocol
	wss	use the WebSocket protocol (SSL/TLS)
	fio-extension	use file I/O extension (beta, Linux)
	fio-direct	use Direct I/O (beta, Linux)
	fio-async-linux	use Linux asynchronous I/O (beta, Linux)
V	version	display the version
	config-test	display the loaded outcome of input parameters and configuration file
	system-info	show system info
	run-host-benchmark	run host benchmark
	run-host-benchmark-categories	specify measurement categories on the benchmark
h	help	the display command line help
m	copy-mode	copy mode
o	overwrite	overwrite mode
a	fail-action	set the behavior when processing a file fails
	user	user name
	password	password
f	sourcefile	source file list
	source-file-host	set the remote host (in use of the source file)
	port	set the remote port (in use of the source file)
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	hcp-out	specify the file to output execution results
	investigation	investigation mode
	multi-run	Multiple run mode
	no-diskio-keep-read	no disk I/O, but keep reading
	no-diskio-keep-write	no disk I/O, but keep writing
	no-diskio-keep-	no disk I/O and Direct I/O, but keep malloc

Bytix Archaea tools Command Reference

	memalign	with alignment
	no-skip-hcp-file	Disable skipping HCP files in transfer
	no-integrity-on-resume	Disable integrity check on resume
	no-agent	don't use agent
	ident-select	select identity
	overwrite-als-temp-file	atomically overwrite a temporary file
	preserve-win-read-only	preserve read-only attributes of Windows files and folders
	udp	use the UDP (HpFP) protocol (bi-port form of HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	fio-direct-align	alignment size on Direct I/O
	fio-direct-align-local	alignment size on source site
	fio-direct-align-remote	alignment size on destination site
	fio-direct-malloc	how to malloc with alignment
	fio-direct-reuse-aligned	reuse allocated memory with alignment
	fio-direct-threshold	threshold of files for Direct I/O
	fio-async-max-events	maximum events of asynchronous I/O
	fio-async-max-get-events	maximum events to get on asynchronous I/O

	fio-async-get-events-timeo	timeout on getting events on asynchronous I/O
	fio-fallocate	how making pre-allocation of storage
	fio-fallocate-unit	unit size of the pre-allocation
	fio-no-extension-read	suppress file I/O extension on source site
	fio-no-extension-write	suppress file I/O extension on destination site
	fio-extension-always	force file I/O extension for all files
	reading-dev	read from special devices sequentially
	reading-dev-via-mmap	read from the special devices via mapped I/O
	transfer-expire	set the transfer expiration
	no-out-of-order-header-messaging	suppressing out-of-order of control messages
	mcd	set the number of maximum connections per session
	auto-resume	automatically resume
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

1.3.1 p, permission

```
=====
Supported OS : Linux / Windows / Mac
Format : -p | --permission
=====
```

The file permission from the source (UID/GID, the flag with the execution right and so on) and file attributes (modification date and so on) are stored in the destination. When the permission and file attributes can't be stored in the destination due to the access right, the attributes applied by OS when written in the file are kept.

--

Example :

```
[user@localhost ~]$ hcp -p ...  
--
```

1.3.2 R, recursive

```
=====
Supported OS : Linux / Windows / Mac
Format : -R | --recursive
=====
```

The directory from source is searched recursively and the file is transferred.

```
--
Example :
[user@localhost ~]$ hcp -R ...
--
```

1.3.3 Y, anydirs

```
=====
Supported OS : Linux / Windows / Mac
Format : -Y | --anydirs
=====
```

In the case that pattern matching is set by regex option or wildcard, directory search is carried out ignoring the pattern matching.

```
--
Example :
[user@localhost ~]$ hcp -Y ...
--
```

1.3.4 g, regex

```
=====
Supported OS : Linux / Windows / Mac
Format : -g | --regex
=====
```

The path from source is regarded as a regular expression. The path from source is regarded as a pattern string including wildcard (*) when no use of the option.

When specified path from source is not found as a directory or a file, verification by regular expression is carried out. In searching files, the names of files and directories are verified in this way. Files and directories which doesn't match the pattern is skipped. Pattern strings is chosen from the strings after the last path delimiter ("/").

```
--
Example :
[user@localhost ~]$ hcp -g ...
--
```

1.3.5 y, verify

```
=====
Supported OS : Linux / Windows / Mac
Format : -y | --verify
=====
```

Data blocks and files to send are verified by message digest.

```
--
Example :
[user@localhost ~]$ hcp -y ...
--
```

1.3.6 z, compress

```
=====
Supported OS : Linux / Windows / Mac
Format : -z | --compress
=====
```

Data blocks to send are compressed.

```
--
Example :
[user@localhost ~]$ hcp -z ...
--
```

1.3.7 s, copy-linkfile

```
=====
Supported OS : Linux / Windows / Mac
Format : -s | --copy-linkfile
=====
```

hcp copies files that a symbolic link refers. A symbolic link is created in the destination, when this option is not used.

```
--
Example :
[user@localhost ~]$ hcp -s ...
--
```

1.3.8 S, follow-linkdir

```
=====
Supported OS : Linux / Windows / Mac
Format : -S | --follow-linkdir
=====
```

hcp searches the directories that a symbolic link refers.

It should be noted that much data processing may happen with using this option, which is not unexpected with the information (number of files and their total size) got from the source path without resolving cyclic directory searches or its link.

--

Example :

```
[user@localhost ~]$ hcp -S ...
```

--

1.3.9 H, dereference-src

```
=====
Supported OS : Linux / Windows / Mac
Format : -H | --dereference-src
=====
```

hcp makes dereference of symbolic links specified on SOURCE to copy files and directories.

--

Example :

```
[user@localhost ~]$ hcp --dereference-src ...
```

--

1.3.10 e, no-emptyfile

```
=====
Supported OS : Linux / Windows / Mac
Format : -e | --no-emptyfile
=====
```

hcp dose not copy empty files.

--

Example :

```
[user@localhost ~]$ hcp -e ...
```

--

1.3.11 E, no-emptydir

```
=====
Supported OS : Linux / Windows / Mac
Format : -E | --no-emptydir
=====
```

hcp dose not copy empty directories that have no files and no directories.

--

Example :

```
[user@localhost ~]$ hcp -E ...
```

--

1.3.12 d, no-dotfile

```
=====
Supported OS : Linux / Windows / Mac
Format : -d | --no-dotfile
=====
```

hcp dose not copy files whose name starts with “.”.

```
--
Example :
[user@localhost ~]$ hcp -d ...
--
```

1.3.13 D, no-dotdir

```
=====
Supported OS : Linux / Windows / Mac
Format : -D | --no-dotdir
=====
```

hcp dose not copy directories whose name starts with “.”.

```
--
Example :
[user@localhost ~]$ hcp -D ...
--
```

1.3.14 I, copy-hidden

```
=====
Supported OS : Windows
Format : -I | --copy-hidden
=====
```

hcp copies hidden files.

```
--
Example :
[user@localhost ~]$ hcp -I ...
--
```

1.3.15 A, archive-check

```
=====
Supported OS : Windows
Format : -A | --archive-check
=====
```

hcp copies files having archive attributes.

When the destination OS is Windows including the case when this option isn't set, the archive attribute is set at the right time following the OS behavior.(This software doesn't set any archive attribute configurations even when creating a new file and updating.)

--

Example :

```
[user@localhost ~]$ hcp -A ...
```

--

1.3.16 sparse

```
=====
Supported OS : Linux / Windows / Mac
Format : --sparse
=====
```

This option tells hcp to transfer some sparse (including holes) files with detecting holes and reproducing them at writing.

If you do not use this option, the holes will be padded with zero data in the transfer.

--

Example :

```
[user@localhost ~]$ hcp --sparse ...
```

--

1.3.17 q, quiet

```
=====
Supported OS : Linux / Windows / Mac
Format : -q | --quiet
=====
```

Suppress non-error message outputs.

--

Example :

```
[user@localhost ~]$ hcp -q ...
```

--

1.3.18 r, resume

```
=====
Supported OS : Linux / Windows / Mac
Format : -r <run-record-path> | --resume=<run-record-path>
-----
run-record-path
Default : none
Range of Values : path string of file system
=====
```

hcp restarts file operations with the execution records (the forwarding execution records output in .hcp.out).

```
--
Example :
[user@localhost ~]$ hcp ...
[user@localhost ~]$ mv .hcp.out .hcp.in
[user@localhost ~]$ hcp -r .hcp.in ...
--
```

When a file exists on its destination, an integrity check will be performed if content of the file is same as a head of the corresponding file on the source. If it is, then resuming will be performed. And if it is not, transfer of the file starts with its head.

For disabling this integrity check, please use `—no-integrity-on-resume`.

1.3.19 N, no-send

```
=====
Supported OS : Linux / Windows / Mac
Format : -N | --no-send
=====
```

hcp runs without transferring data to the network.

This option is used to confirm the disk I/O at source and the performance of data processing.

```
--
Example :
[user@localhost ~]$ hcp -N ...
--
```

1.3.20 n, no-diskio

```
=====
Supported OS : Linux / Windows / Mac
Format : -n <bench_spec> | --no-diskio=<bench_spec>
      bench_spec := <number_of_files>:<file_size>
-----
```

```
number_of_files
Default : none
Range of Values : unsigned integer
-----
```

```
file_size
Default : none
Range of Values : unsigned double-length integer
=====
```

hcp runs without performing local I/O at source and destination.

This option is used to check the network transmission performance. Each meanings of the option parameter are below.

`number_of_files` := the number of files to transfer
`file_size` := the size to transfer files (byte)

When the option is "0:0", the sender path is searched as the normal operation and the file is transferred.(References of file attributes for the permission option and reading data of files are not carried out.)

This option is available even when `/dev/zero` is specified at the destination. In this case, it practically reads, transfers and writes the data from `/dev/zero` to the destination, whose size is specified by `file_size` in this option. Unlike the behavior described above, the I/O processing is not omitted. This option is typically used to check the transmission performance by specifying `/dev/null` at the destination and adding read/write by special devices.

```
--
Example1 :
[user@localhost ~]$ hcp -n 1000:1048576 ...
Example2 :
[user@localhost ~]$ hcp -n 1:1048576 /dev/zero 192.168.10.100:874:/dev/nu
ll
--
```

1.3.21 hpfp

```
=====
Supported OS : Linux / Windows / Mac
Format : --hpfp
=====
```

It instructs transport to use HpFP protocol.

```
--
Example :
[user@localhost ~]$ hcp ... --hpfp /path/to/src_file 192.168.10.100:6552
0:/path/to/dst_file
--
```

1.3.22 wss

```
=====
Supported OS : Linux / Windows / Mac
Format : --wss
=====
```

It instructs transport to use WebSocket protocol (SSL/TLS).

--

Example :

```
[user@localhost ~]$ hcp ... --wss /path/to/src_file 192.168.10.100:443:/path/to/dst_file
```

--

1.3.23 fio-extension

```
=====
Supported OS : Linux (beta)
Format : --fio-extension
=====
```

This option tells the hcp command to use file I/O extension for reading and writing files.

When this option is specified, the following configuration will be applied.

- Direct I/O and Linux asynchronous I/O
- Direct I/O alignment auto detection
- Direct I/O threshold 1GB
- Asynchronous I/O maximum events 32
- Storage pre-allocation native/256MB

--

Example :

```
[user@localhost ~]$ hcp --fio-extension 1GB.src.dat 192.168.10.100:1GB.dst.dat
```

--

1.3.24 fio-direct

```
=====
Supported OS : Linux (beta)
Format : --fio-direct
=====
```

This option tells the hcp command to use Direct I/O for reading and writing files. The fio-extension will be implied (no need to specify it explicitly).

Please use this option when you want to use only Direct I/O without Linux asynchronous I/O.

--

Example :

```
[user@localhost ~]$ hcp --fio-direct 1GB.src.dat 192.168.10.100:1GB.dst.d
```

at
--

1.3.25 fio-async-linux

```
=====
Supported OS : Linux (beta)
Format : --fio-async-linux
=====
```

This option tells the hcp command to use Linux asynchronous I/O for reading and writing files. The fio-direct will be implied (no need to specify it explicitly).

Please use this option when you want to specify it explicitly.

When a writing process is crashed (unexpectedly stopped) using this option and an option for pre-allocation of storage (fio-fallocate option described below), resuming transfer (using the resume option) might start with the head of a file (new transfer).

This option cannot be used with the sparse option. Running command will be stopped with an error if you do it.

```
--
Example :
[user@localhost ~]$ hcp --fio-async-linux 1GB.src.dat 192.168.10.100:1GB.
dst.dat
--
```

1.3.26 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hcp command version is shown.

```
--
Example :
[user@localhost ~]$ hcp -V
hcp client (hcp) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS 4.
2.0-2)
--
```

1.3.27 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

Bytix Archaea tools Command Reference

The hcp command parameters and configuration parameters are shown.

```
--
Example :
[user@localhost ~]$ hcp --config-test
...

-- [Sources] -----
---
-- [Destination] -----
---
-- [Command Options] -----
---
permission      : disable
recursive       : disable
anydirs         : disable
regex          : disable
verify         : disable
compress       : disable
copy-linkfile   : disable (don't copy symlink file)
follow-linkdir  : disable (don't follow symlink directory)
dereference-src : disable
no-emptyfile   : disable (copy)
no-emptydir    : disable (copy)
no-dotfile     : disable (copy)
no-dotdir      : disable (copy)
copy-hidden    : disable (don't copy)
archive-check  : disable (don't check archive property)
resume         : disable
no-send        : disable
no-diskio      : disable
copy-mode      : - [ALLCOPY]
overwrite      : - [FORCE]
fail-action    : - [HALT]
source-file    : -
source-file-host : -
port           : -
quiet          : disable
auto-resume    : disable
user           : -
password       : -
version        : disable
help           : disable
mcd            : -
-- [Configuration Parameters] -----
---
AtomicLikeSaving      : no .tmp NONE [threshold=0]
```

```

PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication       : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts  : 3
CompressLevel            : -1
StrictHostKeyChecking    : ask
IdentityFile             : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.ssh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519 ]
MaxReceiveRate           : 100000000000
MaxSendRate              : 100000000000
MaxConnectionReceiveRate : 100000000000
MaxConnectionSendRate    : 100000000000
TransportTimeout         : 180 sec
FileLock                 : no
AcceptableCryptMethod    : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod   : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER          : user
LOGNAME       : user
HCP_PASSWORD  :
HCP_WS_PROXY  :
-----
---
```

Please type '--config-test --config-test ...' for more details.

--

If you want to confirm more detailed configuration options, please add `—config-test` (other client commands are also in the same manner to show).

1.3.28 system-info

```

=====
Supported OS : Linux / Windows / Mac
Format : --system-info
=====
```

This option tells hcp to show the system information. The following contents will be displayed.

- CPU brand name
- Number of physical processors and logical processors
- Hardware acceleration information around AES function

Bytix Archaea tools Command Reference

- System memory size
- Kernel information (Linux / Mac)
- OS information
- Host name

When specifying this option twice, the following contents will be displayed.

- Disk consumption (df output, Linux / Mac)
- Network interface detail

--

Example :

```
[user@localhost ~]$ hcp --system-info ...
```

--

1.3.29 run-host-benchmark

```
=====
Supported OS : Linux / Windows / Mac
Format : --run-host-benchmark
=====
```

This option tells hcp to make a benchmark of the local host about the following performances.

- Security communication performance (AES, GCM/CTR/CBC mode, MD5, SHA1, SHA256)
- File integrity validation performance (XXH3, Parity)
- Disk reading & writing performance (Cached, Direct I/O)
- Memory copy performance

When this option is specified twice, the benchmark run with some additional conditions.

- Security communication performance (some additional AES benchmarks around block size and concurrency)
- File integrity validation performance (some additional benchmarks about Parity calculation)
- Disk reading & writing performance (some additional benchmarks around block size)
- Memory copy performance (an additional benchmark on concurrency)

Benchmarks using Direct I/O and additional disk benchmarks are available only for Linux version.

--

Example :

```
[user@localhost ~]$ hcp --run-host-benchmark ...
```

--

1.3.30 run-host-benchmark-categories

```
=====
Supported OS : Linux / Windows / Mac
Format : --run-host-benchmark-categories=<categories>
-----
categories
Default : all
Range of Values : secure, integrity, disk, memory, all
=====
```

You can specify measurement categories over which hcpd make the benchmark. The following values are available.

- secure (security communication performance)
- integrity (file integrity validation performance)
- disk (disk reading & writing performance)
- memory (memory copy performance)
- all (all of the values above)

Please use this option to reduce measurements when it takes a long time.

--

Example :

```
[user@localhost ~]$ hcp --run-host-benchmark-categories=disk,memory ...
```

--

1.3.31 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The help information on the hcp commands is shown.

--

Example :

```
[user@localhost ~]$ hcp -h
--
```

1.3.32 m, copy-mode

```
=====
Supported OS : Linux / Windows / Mac
Format : -m <mode_name> | --copy-mode=<mode_name>
-----
mode_name
Default : ALLCOPY
Range of Values : ALLCOPY, UPDATE, DIFF, DIFF_STRICT, SYNC
=====
```

The file copy mode is set.

ALLCOPY means copying all files.

In the UPDATE mode, the source file and the destination file are compared and when the source file is newer than the destination one, hcp copies the source file.

In the DIFF mode, the file size is also compared in addition to UPDATE.

In the DIFF_STRICT mode, the hashes of files are also compared in addition to DIFF.

In the SYNC mode, the destination file which doesn't exist in the source, is deleted.(synchronization)

```
--
Example :
[user@localhost ~]$ hcp -m UPDATE ...
--
```

1.3.33 o, overwrite

```
=====
Supported OS : Linux / Windows / Mac
Format : -o <overwrite_name> | --overwrite=<overwrite_name>
-----
overwrite_name
Default : FORCE
Range of Values : CONFIRM, FORCE, RENAME, BACKUP
=====
```

As for overwriting, the mode is set.

The CONFIRM mode overwrites with confirmation.

The FORCE mode overwrites without confirmation.

The RENAME mode renames the file by adding a following suffix on the original file names before overwriting..

.YYMMDD_HHMMSS.NNN (NNN are the sequence numbers)

The BACKUP mode moves the original file to the following backup directory before overwriting.

./YYMMDD_HHMMSS/

The directory name is created in the unique process during transactions.

--

Example :

```
[user@localhost ~]$ hcp -o CONFIRM ...
```

--

1.3.34 a, fail-action

```
=====
Supported OS : Linux / Windows / Mac
Format : -a <action_name> | --fail-action=<action_name>
-----
action_name
Default : HALT
Range of Values : HALT, SKIP
=====
```

The behavior in the case of file copy errors is set.

When some problems happen in file copying,The HALT mode stops the copy.

When some problems happen in file copying,The SKIP mode skips that file and keeps copying the next possible files.

--

Example :

```
[user@localhost ~]$ hcp -a SKIP ...
```

--

1.3.35 user

```
=====
Supported OS : Linux / Windows / Mac
Format : --user=<username>
-----
username
Default : none
Range of Values : user name
=====
```

The user name for user authentication is set.

```
--  
Example :  
[user@localhost ~]$ hcp --user=user ...  
--
```

1.3.36 password

```
=====
Supported OS : Linux / Windows / Mac
Format : --password=<password>
-----
password
Default : none
Range of Values : password
=====
```

The user credentials (password and pass-phrase) for user authentication are set.

```
--  
Example :  
[user@localhost ~]$ hcp --password=password ...  
--
```

1.3.37 f, source-file

```
=====
Supported OS : Linux / Windows / Mac
Format : -f <source-path-list-file> | --source-file=<source-path-list-file>
-----
source-path-list-file
Default : none
Range of Values : path string of file system
=====
```

It specifies the file including a list of the source.

```
--  
Example1 : In the case of the source is localhost.
```

```
[user@localhost ~]$ cat source.list
file1.txt
child_dir/file2.txt
child_dir2/
/home/user/file3.txt

[user@localhost ~]$ hcp -f source.list ...
```

--

Example2 : In the case of the source 1 is remote host.

```
[user@localhost ~]$ cat source.list
192.168.100.100:874:file1.txt
:child_dir/file2.txt
:child_dir2/
:/home/user/file3.txt
```

```
[user@localhost ~]$ hcp -f source.list ...
```

--

Example3 : In the case of the source 2 is remote host.

```
[user@localhost ~]$ cat source.list
file1.txt
child_dir/file2.txt
child_dir2/
/home/user/file3.txt
```

```
[user@localhost ~]$ hcp -f source.list --source-file-host=127.0.0.1 ...
```

--

Example4 : In the case of the source 3 is remote host.

```
[user@localhost ~]$ cat source.list
192.168.100.100:874:file1.txt
192.168.100.100:874:child_dir/file2.txt
192.168.100.100:874:child_dir2/
192.168.100.100:874:/home/user/file3.txt
```

```
[user@localhost ~]$ hcp -f source.list ...
```

--

1.3.38 source-file-host

```
=====
Supported OS : Linux / Windows / Mac
Format : --source-file-host=<remote-host>[:<remote-port>]
-----
remote-host
Default : none
Range of Values : IP address or hostname
-----
remote-port
Default : none
Range of Values : port number
=====
```

It specifies a remote host for the source-file option.

```
--  
Example :  
[user@localhost ~]$ hcp --source-file-host=192.168.100.100 ...  
--
```

1.3.39 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
remote-port
Default : none
Range of Values : port number
=====
```

It specifies a service port number of the remote host in the destination. When — source-file-host is used, this port is effective.

```
--  
Example :  
[user@localhost ~]$ hcp --port=1874 ...  
--
```

1.3.40 config-file

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-file=<config-file-path>
-----
config-file-path
Default : none
Range of Values : path string of file system
=====
```

The configuration file path used for the hcp command is set.

The hcp commands read the configuration files in the following order.

1. /etc/hcp/hcp.conf
2. <user home directory>/.hcp/hcp.conf
3. <the path configured in the options>

When the file doesn't exist, it is skipped. When the configuration file wasn't read successfully, file read error occurs and the operation stops.

```
--  
Example :
```

```
[user@localhost ~]$ hcp --config-file=hcp.conf ...  
--
```

1.3.41 config-option

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-option=<config-file-option-desc>
-----
config-file-option-desc
Default : none
Range of Values : description of a configuration item described in config
uration files
=====
```

This option tells the hcp command to apply a configuration item from the command line parameters instead of using configuration files.

The configuration item will be applied at last after other configuration files are loaded.

```
--
Example :
[user@localhost ~]$ hcp --config-option="DiagnosticLog DEBUG" ...
--
```

1.3.42 show-config-options

```
=====
Supported OS : Linux / Windows / Mac
Format : --show-config-options
=====
```

This option tells the hcp command to show available option names of its configuration.

```
--
Example :
[user@localhost ~]$ hcp --show-config-options ...
--
```

1.3.43 hcp-diag

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-diag=<log-file-path>
-----
log-file-path
Default : none
Range of Values : path string of file system
=====
```

The hcp command log for diagnostic is output in the file with the path configured.

Bytix Archaea tools Command Reference

```
--  
Example :  
[user@localhost ~]$ hcp --hcp-diag=hcp.log ...  
--
```

The old name of 'log-file' is available.

1.3.44 stat-log-file

```
=====
Supported OS : Linux / Windows / Mac
Format : --stat-log-file=<log-file-path>
-----
log-file-path
Default : none
Range of Values : path string of file system
=====
```

The standard path for the statistics log output by the hcp commands is set.

Each statistics log is output in the configured path with suffixes.

```
<conigured path>.application (application statistics)
<conigured path>.transport.tcp (TCP transport statistics)
<conigured path>.transport.hpfp (HpFP transport statistics)
<conigured path>.transport.ws (WS/WSS transport statistics)
```

```
--
Example :
[user@localhost ~]$ hcp --stat-log-file=.hcp.statistics2 ...
--
```

1.3.45 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to record transmission execution results is set. The output information by this option is used in the resume option.

```
--
Example :
[user@localhost ~]$ hcp --hcp-out=- ...
SRC /home/user/Desktop/hcp_src5
```

Bytix Archaea tools Command Reference

```
DST 127.0.0.1:11112:/home/user/Desktop/hcp_dst5
OK 0000 FS 80000001 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FT 00000001 /home/user/Desktop/hcp_src5/file1.txt
EXIT 0 REASON 0000
--
```

If this option is not specified, execution records are stored in the following files, etc., in the execute directories.

```
.hcp.out (Linux)
_hcp.out (Windows)
```

When “-” is set, execution records are output as the standard output.

FT (File Transfer) shows procedures for file transfer, which format is below.

```
<result> <reason> FT <sequence> [<src_label> ]<path>
```

shows processing results, either OK or NG.

shows reason_code (described later), which explains the reason for the result.

is the sequence number for the processing.

is the source label corresponding to the file used in each processing. The format is below.

```
SRC<src_index>
```

is the index of the source specified.

shows the file path used in the processing, which is the path of the host executing the command.

When multiple sources are specified, progress information is recorded as below.

Example :

```
SRC0 /home/user/Desktop/hcp_src5
SRC1 /home/user/Desktop/hcp_src6
DST 127.0.0.1:11112:/home/user/Desktop/hcp_dst5
OK 0000 FS 80000001 SRC0 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FS 80000002 SRC0 /home/user/Desktop/hcp_src5/file2.txt
OK 0000 FS 80000003 SRC1 /home/user/Desktop/hcp_src6/file3.txt
OK 0000 FS 80000004 SRC1 /home/user/Desktop/hcp_src6/file4.txt
OK 0000 FT 00000001 SRC0 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FT 00000002 SRC0 /home/user/Desktop/hcp_src5/file2.txt
OK 0000 FT 00000003 SRC1 /home/user/Desktop/hcp_src6/file3.txt
OK 0000 FT 00000004 SRC1 /home/user/Desktop/hcp_src6/file4.txt
```

Bytix Archaea tools Command Reference

EXIT 0 REASON 0000

—

FS (File Sync) shows file synchronization processing. When the synchronization deletes files in the destination that don't exist on the source host, the following text is recorded.

—

Example :

```
SRC /home/user/Desktop/hcp_src5
DST 127.0.0.1:11112:/home/user/Desktop/hcp_dst5
OK 0000 FS 80000001 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FS 80000002 /home/user/Desktop/hcp_src5/file2.txt
OK A001 FS 80000003 /home/user/Desktop/hcp_src5/file3.txt
OK 0000 FT 00000001 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FT 00000002 /home/user/Desktop/hcp_src5/file2.txt
EXIT 0 REASON 0000
```

—

When a file cannot be identified in a single source, the index of the source label is shown by "?."

—

Example :

```
SRC0 /home/user/Desktop/hcp_src5
SRC1 /home/user/Desktop/hcp_src6
DST 127.0.0.1:11112:/home/user/Desktop/hcp_dst5
OK 0000 FS 80000001 SRC0 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FS 80000002 SRC0 /home/user/Desktop/hcp_src5/file2.txt
OK 0000 FS 80000003 SRC1 /home/user/Desktop/hcp_src6/file3.txt
OK 0000 FS 80000004 SRC1 /home/user/Desktop/hcp_src6/file4.txt
OK A001 FS 80000005 SRC? /home/user/Desktop/hcp_src6/file5.txt
OK 0000 FT 00000001 SRC0 /home/user/Desktop/hcp_src5/file1.txt
OK 0000 FT 00000002 SRC0 /home/user/Desktop/hcp_src5/file2.txt
OK 0000 FT 00000003 SRC1 /home/user/Desktop/hcp_src6/file3.txt
OK 0000 FT 00000004 SRC1 /home/user/Desktop/hcp_src6/file4.txt
EXIT 0 REASON 0000
```

—

In the last line, and are recorded in the following format.

EXIT <exit_status> REASON <reason_code>

When the setting, UseProperCopyAndSync described later is set as yes, on searching a directory, the judging result on overwriting is recorded in the following format.

<result> <reason> DE <sequence> [<src_label>]<path>

1.3.46 multi-run

Supported OS : Linux / Windows / Mac

Format : --multi-run=<record-path>[:<output-switch>]

record-path

Default : none

Range of Values : path string of file system

output-switch

Format : ((A|T|R|L)[...] | THRU | FULL)

Default : THRU

A client starts in the multiple run mode. With this option, the following logs are recorded in unique file names in the specified directory. It is used when plural clients access to the same directory simultaneously or executing another applications is taken place in the background.

- Application statistics
- Transport statistics
- Result output
- Application log

record-path specifies the directory of these log files.

output-switch specifies the control of these logs outputs.

A stands for the application statistics. With this option, the application statistics is recorded in the following file name in the directory specified above.

hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.statistics.application

T stands for the transport statistics. With “T”,the transport statistics is recorded in the following file name in the above directory.

hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.statistics.transport.<protocol>

R stands for the execution result. With “R”,the execution result is recorded in the following file name in the above specified directory.

hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.out

L stands for the application log. With “L”,the application log is recorded in the following file name in the above specified directory.

hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.log

With “FULL”, the behavior is the same as one with “ATRL”.

With “THRU”, outputs of the records are processed following the specifications of the configuration files and commands. When the application statistics (transport statistics) in the configuration file is enable, it is recorded in the above file name. When the result output (the application log) is enable (without -v and with -l), the execution record (log) is output in the above file name.

--

Example :

```
[user@localhost ~]$ hcp --multi-run=/var/tmp:ATR // The log is output as
standard. Other files are output in /var/tmp.
```

--

1.3.47 no-diskio-keep-read

```
=====
Supported OS : Linux / Windows / Mac
Format : --no-diskio-keep-read
=====
```

When hcp runs without performing local I/O at source and destination (-n option), this option tells it to perform reading data from the source.

This option is exclusive with —no-diskio-keep-write.

It is useful for making investigation to break down causes in cases where reading data on disk I/O is supposed to be a performance bottleneck.

1.3.48 no-diskio-keep-write

```
=====
Supported OS : Linux / Windows / Mac
Format : --no-diskio-keep-write
=====
```

When hcp runs without performing local I/O at source and destination (-n option), this option tells it to perform writing data to the destination.

This option is exclusive with —no-diskio-keep-read.

It is useful for making investigation to break down causes in cases where writing data on disk I/O is supposed to be a performance bottleneck.

1.3.49 no-diskio-keep-memalign

```
=====
Supported OS : Linux
```

Format : --no-diskio-keep-memalign

When hcp runs without performing local I/O at source and destination (-n option) and runs with Direct I/O, this option tells it to perform memory allocation with alignment for buffers holding payloads of files.

It is useful for making investigation to break down causes in cases where loads of making memory allocation with alignment is supposed to be a performance bottleneck.

1.3.50 no-skip-hcp-file

Supported OS : Linux / Windows / Mac

Format : --no-skip-hcp-file

In default, hcp becomes skipping the following files from its file transfer. This option will disable this skipping function.

- Linux/macOS : .hcp.out, .hcp.in, .hcp.diag, .hcp.statistics.*
- Windows : _hcp.out, _hcp.in, _hcp.diag, _hcp.statistics.*

1.3.51 no-integrity-on-resume

Supported OS : Linux / Windows / Mac

Format : --no-integrity-on-resume

This option disables an integrity check of a file on resume. Just detection of resuming position will be performed for files on its destination.

It is useful for reducing processing time in cases where the integrity check takes long time because of the following reasons.

- Machine performance is worse
- A size of a partial file for resume is too huge

1.3.52 no-agent

Supported OS : Linux / Windows / Mac

Format : --no-agent

This option tells clients not to use key agents such as ssh-agent and pageant on public key authentication.

This is useful for avoiding authentication failures in some cases where you do not want to use keys that are loaded in the agents or the old servers do not support them.

Clients will work as if this option is specified when the agents is not working in user environments or any key is not loaded on them.

1.3.53 ident-select

```
=====
Supported OS : Linux / Windows / Mac
Format : --ident-select=<path-desc>
```

```
-----
path-desc
Default : not defined
Range of Values : A path string in file system
=====
```

This option tells clients to select a file holding a private key by the given path description.

This is useful for specifying a particular private key to use for public key authentication when another key is detected and its authentication by the another key meets a failure.

1.3.54 overwrite-als-temp-file

```
=====
Supported OS: Linux / Windows / Mac
Format : --overwrite-als-temp-file
=====
```

It requests to overwrite a temporary file which already exists.

Without this option, the transferring file goes to the transfer error when a temporary file already exists.

As long as AtomicLikeSavingRejectOverwriteRequest is set to yes in the server setting, even though this option is on, overwriting a temporary file which already exists is rejected.

1.3.55 preserve-win-read-only

```
=====
upported OS: Linux / Windows
Format : --preserve-win-read-only
=====
```

The read-only attribute on Windows in the destination is kept. It is applied when the read-only attribute on Windows in the destination is enabled, or Unix owners have only read access.

1.3.56 udp

```
=====
Supported OS : Linux / Windows / Mac
Format : --udp=<hpfp_options>
  hpfp_options := <hpfp_udp_port>:<hpfp_cong_mode>:<hpfp_sndbuf>:<hpfp_rcv
buf>:<hpfp_mss>
-----
hpfp_udp_port
Format : ( DEFAULT | D | <decimal_number> )
Default : 65520
Range of Values : decimal_number is 1 - 65535. D stands for DEFAULT
-----
hpfp_cong_mode
Default : FAIR
Range of Values : DEFAULT (D) , FAIR (F) , MODEST (M) , FAIR_FAST_START
(S) , AGGRESSIVE (A)
  () is abbreviated notation.
-----
hpfp_sndbuf
Format : ( DEFAULT | D | <decimal_number>[[ (T|G|M|K)]B] )
Default :
  100MB (Linux.x86 / Windows / Mac)
  8MB (Raspbian)
Range of Values : unsigned double-length integer in byte. D stands for DE
FAULT.
-----
hpfp_rcvbuf
Format : ( DEFAULT | D | <decimal_number>[[ (T|G|M|K)]B] )
Default :
  200MB (Linux.x86 / Windows / Mac)
  16MB (Raspbian)
Range of Values : unsigned double-length integer in byte. D stands for DE
FAULT.
-----
hpfp_mss
Format : ( DEFAULT | D | NONE | N | <decimal_number>[[ (T|G|M|K)]B] )
Default : NONE
Range of Values : unsigned integer (byte) D stands for DEFAULT. N stands
for NONE.
=====
```

This option is going to be deprecated.

It instructs transport to use HpFP protocol.

hpfp_udp_port specifies the UDP port number used in HpFP protocol.

hpf_p Cong_mode specifies congestion control mode.

The sending buffer size of the HpFP protocol is set in hpf_p_sndbuf in bytes.

The receiving buffer size of the HpFP protocol is set in hpf_p_rcvbuf in bytes.

The MSS (Maximum Segment Size) of the HpFP protocol is set in hpf_p_mss. The best size is the size of the MTU size minus 44 bytes of the protocol header. "N (NONE)" means none specified. When it's "D", the default value is used. when "N", it is decided by the MTU search in HpFP protocol.

Regarding congestion control mode, if the server doesn't accept the mode, FAIR is applied. When different algorithm that user isn't meant to is applied by this operation, which is notified by the following log.

```
2018/07/05 13:20:44 00007f9a2dfa0700:INFO :Your requested congestion mode
of HpFP will not be used (requested=AGGRESSIVE, actual=FAIR).
```

--

Example :

```
[user@localhost ~]$ hcp --udp=D:S:4MB:8MB:8956B ...
```

--

1.3.57 ws

```
=====
Supported OS : Linux / Windows / Mac
Format : --ws
=====
```

It instructs transport to use the WebSocket protocol (cleartext).

1.3.58 wss-no-check-certificate

```
=====
Supported OS : Linux / Windows / Mac
Format : --wss-no-check-certificate
=====
```

It instructs not to check server certificates when SSL/TLS in the WebSocket protocol is used. As a result, it receives server certificates without checking the CN (Common Name), expiration, intermediate certificate, and root certificate.

1.3.59 ws-proxy-direct

```
=====
Supported OS : Linux / Windows / Mac
Format : --ws-proxy-direct
=====
```

It instructs not to use proxy servers when the WebSocket protocol is used.

1.3.60 ws-proxy

```
=====
Supported OS : Linux / Windows / Mac
Format : --ws-proxy=<proxy_server>
-----
proxy_server
Format : <proxy_server_address>:<proxy_server_port_number>
Default : none
Range of Values : proxy server address and port number
=====
```

A proxy server for the WebSocket protocol is specified, which is applied regardless of whether SSL/TLS is used. When it is not specified, it follows the system proxy setting.

1.3.61 hpfp-cong

```
=====
Supported OS : Linux / Windows / Mac
Format : --hpfp-cong=<hpfp_cong_mode>
-----
hpfp_cong_mode
Default : FAIR
Range of Values : FAIR(F), MODEST(M), FAIR_FAST_START(S), AGGRESSIVE(A)
() is abbreviated notation.
=====
```

The congestion control mode for the HpFP protocol is set.

In the case that a server doesn't accept the specified congestion control mode, FAIR is set and the following log is output.

```
2018/07/05 13:20:44 00007f9a2dfa0700:INFO :Your requested congestion mode
of HpFP will not be used (requested=AGGRESSIVE, actual=FAIR).
```

--

Example :

```
[user@localhost ~]$ hcp ... --hpfp --hpfp-cong=S /path/to/src_file 192.16
8.10.100:65520:/path/to/dst_file
```

--

1.3.62 hpfp-mss

```
=====
Supported OS : Linux / Windows / Mac
Format : --hpfp-mss=<hpfp_mss>
-----
hpfp_mss
Format : ( NONE | N | <decimal_number>[[ (T|G|M|K)]B] )
Default : NONE
```

Range of Values : unsigned integer (byte) N stands for NONE.

MSS (Maximum Segment Size) for the HpFP protocol is set. MTU minus 44 bytes, the protocol header, is the optimal value. When N is set, the value is set by the MTU search by the HpFP protocol.

--

Example :

```
[user@localhost ~]$ hcp ... --hpfp --hpfp-mss=8956 /path/to/src_file 192.168.10.100:65520:/path/to/dst_file
```

--

1.3.63 hpfp-sndbuf

Supported OS : Linux / Windows / Mac

Format : --hpfp-sndbuf=<hpfp_sndbuf>

hpfp_sndbuf

Format : <decimal_number>[[T|G|M|K)]B]

Default :

100MB (Linux.x86 / Windows / Mac)

8MB (Raspbian)

Range of Values : unsigned double-length integer (byte)

The send buffer size (byte) for the HpFP protocol is set.

--

Example :

```
[user@localhost ~]$ hcp ... --hpfp --hpfp-sndbuf=8MB /path/to/src_file 192.168.10.100:65520:/path/to/dst_file
```

--

1.3.64 hpfp-rcvbuf

Supported OS : Linux / Windows / Mac

Format : --hpfp-rcvbuf=<hpfp_rcvbuf>

hpfp_rcvbuf

Format : <decimal_number>[[T|G|M|K)]B]

Default :

200MB (Linux.x86 / Windows / Mac)

16MB (Raspbian)

Range of Values : unsigned double-length integer (byte)

The receive buffer size (byte) for the HpFP protocol is set.

--

Example :

```
[user@localhost ~]$ hcp ... --hfp --hfp-rcvbuf=16MB /path/to/src_file 1
92.168.10.100:65520:/path/to/dst_file
```

--

1.3.65 fio-direct-align

```
=====
Supported OS : Linux
Format : --fio-direct-align=<alignment>
-----
alignment
Format : <decimal_number>[[(G|M|K)]B]
Default : none
Range of Values : unsigned integer (byte)
=====
```

This option sets an alignment size in bytes of reading and writing buffers for Direct I/O.

When it is not specified or '0' is specified, the hcp command will be looking for a size on the host system (auto detection).

--

Example :

```
[user@localhost ~]$ hcp ... --fio-direct-align=8KB ...
```

--

1.3.66 fio-direct-align-local

```
=====
Supported OS : Linux
Format : --fio-direct-align-local=<alignment>
-----
alignment
Format : <decimal_number>[[(G|M|K)]B]
Default : none
Range of Values : unsigned integer (byte)
=====
```

This option sets an alignment size in bytes on local site (client) for Direct I/O.

Please use this option to specify different sizes on source and destination.

1.3.67 fio-direct-align-remote

```
=====
Supported OS : Linux
```

Format : `--fio-direct-align-remote=<alignment>`

alignment

Format : `<decimal_number>[[G|M|K)]B]`

Default : none

Range of Values : unsigned integer (byte)

=====

This option sets an alignment size in bytes on remote site (server) for Direct I/O.

Please use this option to specify different sizes on source and destination.

1.3.68 fio-direct-malloc

Supported OS : Linux

Format : `--fio-direct-malloc=<how_malloc>`

how_malloc

Default : malloc_h

Range of Values : posix, malloc_h, malloc_f

=====

This option specifies how to make memory allocation with alignment on direct I/O. This will be applied for making allocation of memory area holding data blocks which are created from file payload on file transfer.

When 'posix' is specified, hcp makes that allocation using the standard function of 'posix_memalign'.

When 'malloc_h' is specified, hcp makes that allocation using an implementation which provides an aligned address using the standard function of 'malloc' with saving management information for alignment at its header part.

When 'malloc_f' is specified, hcp makes that allocation using an implementation which provides an aligned address using the standard function of 'malloc' with saving management information for alignment at its footer part.

When using 'posix', the memory allocation performance might be decreased. Please use it when you just need to use the standard function of 'posix_memalign'.

Please use 'malloc_f' as alternative for 'malloc_h' (default) when you do not meet an expected performance using 'malloc_h'.

--

Example :

`[user@localhost ~]$ hcp ... --fio-direct-malloc=posix ...`

--

The old name of 'fio-direct-aligned-malloc' is available.

1.3.69 fio-direct-reuse-aligned

```
=====
Support OS : Linux
Format : --fio-direct-reuse-aligned
=====
```

This option tells hcp to reuse allocated memory area with alignment on direct I/O.

When using this option, hcp make cache of that allocated memory areas with alignment after using them holding data blocks without releasing them for the future data blocks. The capacity of cache is 1GB each running process. When a data block that a cached memory area cannot hold in length is created, that area will be released and hcp makes a new memory area for that block.

Please use this option in cases where reading and writing performance on disks are not expected in 100Gbps environment.

```
--
Example :
[user@localhost ~]$ hcp ... --fio-direct-reuse-aligned ...
--
```

1.3.70 fio-direct-align-threshold

```
=====
Supported OS : Linux
Format : --fio-direct-threshold=<file_size>
-----
file_size
Foramt : <decimal_number>[[ (T|G|M|K)]B]
Default : 1GB
Range of Values : signed double-length integer (byte)
=====
```

This option specifies a threshold in a file size for Direct I/O.

```
--
Example :
[user@localhost ~]$ hcp ... --fio-direct-threshold=2GB ...
--
```

1.3.71 fio-async-max-events

```
=====
Supported OS : Linux
Format : --fio-async-max-events=<max_events>
-----
```

```
max_events
Default : 32
Range of Values : signed integer
=====
```

This option specifies a maximum number of events on asynchronous I/O.

```
--
Example :
[user@localhost ~]$ hcp ... --fio-async-max-events=16 ...
--
```

1.3.72 fio-async-max-get-events

```
=====
Supported OS : Linux
Format : --fio-async-max-get-events=<max_get_events>
-----
```

```
max_get_events
Default : 1
Range of Values : signed integer
=====
```

This option specifies a maximum number of events to get on asynchronous I/O. This changes the maximum number of events to get by calling each 'io_getevents' function.

Please use this option to break down causes in cases where reading and writing performance on disks are not expected in 100Gbps environment.

```
--
Example :
[user@localhost ~]$ hcp ... --fio-async-max-get-events=4 ...
--
```

1.3.73 fio-async-get-events-timeo

```
=====
Supported OS : Linux
Format : --fio-async-get-events-timeo=<timeo>
-----
```

```
timeo
Default : 0
Range of Values : signed double-length integer (microseconds)
=====
```

This option specifies a timeout to get events on asynchronous I/O in microseconds. '0' means disabling the timeout (no timeout).

Please use this option to break down causes around affection of indicating timeouts on calling 'io_getevents' function in cases where reading and writing performance on disks are not expected in 100Gbps environment.

--

Example :

```
[user@localhost ~]$ hcp ... --fio-async-get-events-timeo=1000 ... // time out of 1 milliseconds
```

--

1.3.74 fio-fallocate

```
=====
Supported OS : Linux
Format : --fio-fallocate=<how_allocate>
-----
how_allocate
Default : native
Range of Values : native, standard, none
=====
```

This option tells the hcp command how to make pre-allocation of storage on writing files.

When 'native' is specified, it uses a platform dependent function for the allocation (fallocate on Linux).

When 'standard' is specified, it uses a standard function for the allocation (posix_fallocate on Linux).

When 'none' is specified, any pre-allocation will not be performed.

This option works when using Linux asynchronous I/O.

--

Example :

```
[user@localhost ~]$ hcp ... --fio-async-linux --fio-fallocate=none ...
```

--

1.3.75 fio-fallocate-unit

```
=====
Supported OS : Linux
Format : --fio-fallocate-unit=<alloc_size>
-----
alloc_size
Format : <decimal_number>[[T|G|M|K)]B]
Default : 2560MB
Range of Values : signed double-length integer (byte)
=====
```

This option specifies a unit size of storage pre-allocation on writing files.

--

Example :

```
[user@localhost ~]$ hcp ... --fio-async-linux --fio-fallocate-unit=1GB ...
```

--

1.3.76 fio-no-extension-local

=====

Supported OS : Linux

Format : --fio-no-extension-local

=====

This option disables the file I/O extension on local site (client).

--

Example :

```
[user@localhost ~]$ hcp ... --fio-no-extension-local ...
```

--

1.3.77 fio-no-extension-remote

=====

Supported OS : Linux

Format : --fio-no-extension-remote

=====

This option disables the file I/O extension on remote site (server).

--

Example :

```
[user@localhost ~]$ hcp ... --fio-no-extension-remote ...
```

--

1.3.78 fio-extension-always

=====

Supported OS : Linux

Format : --fio-extension-always

=====

This option tells the hcp command to apply the file I/O extension to all files.

Please use this option to disable the fio-direct-threshold option.

--

Example :

```
[user@localhost ~]$ hcp ... --fio-extension-always ...
```

--

1.3.79 reading-dev

```
=====
Supported OS : Linux / Windows / Mac
Format : --reading-dev
=====
```

It reads data with the read function, when any block devices or character devices are specified at the source.

1.3.80 reading-dev-via-mmap

```
=====
Supported OS : Linux / Windows / Mac
Format : --reading-dev-via-mmap
=====
```

It reads data with Mapped I/O, when any block devices or character devices are specified at the source.

1.3.81 transfer-expire

```
=====
Supported OS : Linux / Windows / Mac
Format : --transfer-expire=<expire_sec>
-----
expire_sec
Default : none
Range of Values : number of seconds until expiration
=====
```

Transferring files will be stopped at the specified second. As long as the file transferring completes in the specified time, it finishes transferring normally.

1.3.82 no-out-of-order-header-messaging

```
=====
Supported OS : Linux / Windows / Mac
Format : --no-out-of-order-header-messaging
=====
```

It suppresses out-of-order of the control message (including file request messages). It unlocks the behaviors such as sending only control messages by the primary connection in the multiple connection mode and the content data (messages including file payload) in the secondary connection. It enables to send all messages in all connections.

1.3.83 mcd

```
=====
Supported OS : Linux / Windows / Mac
Format : --mcd=<multiple_connection_degree>
=====
```

```
-----
multiple_connection_degree
Default : none
Range of Values : 1 - 65535
=====
```

The maximum of the multiple connections is specified. If not specified, it makes connections up to the maximum of the multiple connection setting on the server service. When 1 is set, it transmits by a single connection. In the case of over the maximum connections on the server service, it makes connections up to that.

1.3.84 auto-resume

```
=====
Supported OS : Linux / Windows / Mac
Format : --auto-resume
=====
```

It automatically restarts copying when transmission stops due to network errors. However, in the case that a user stops copying by Ctrl+C, it doesn't restart copying at that time.

It is recommended to use private keys that are not encrypted by passphrases for this purpose. If you need the passphrases, hcp make a cache on the memory of that passphrase to prevent interactive prompts from being shown for re-authentication.

1.3.85 include-conf-from-cwd

```
=====
Supported OS : Linux / Windows / Mac
Format : --include-conf-from-cwd
=====
```

When using Include in a relative path on configuration files, this option enables finding a file with a path relative to the current directory where commands run.

1.3.86 no-earlier-serv-compat

```
=====
Supported OS : Linux / Windows / Mac
Format: --no-earlier-serv-compat
=====
```

This option disables the backward compatibility for servers that will be performed when the connecting servers are earlier than the client. This function is available to work if you do not use some functions. This option disables the function works (earlier version's clients are still available to work with newer version's servers in that condition). Please see the list in the back of this document about what conditions the function works in.

1.4 hsync

Local : hsync [OPTION]... SRC [SRC]... DEST

Remote :

Push : hsync [OPTION]... SRC [SRC]... [USER@]HOST[:PORT]:DEST

Pull : hsync [OPTION]... [USER@]HOST[:PORT]:SRC [:SRC]... DEST

The hsync command is a command that synchronizes files between a remote server and clients. It also supports synchronizing local files.

abbreviation	option	outline
v	verbose	increase log verbosity
	info	set the log verbosity level of INFO
q	quiet	suppress non-error messages
c	checksum	verify transferred files by digest check
a	archive	archive mode is -rlptgoD
r	recursive	recurse into directories
R	relative	use relative path names
	no-implied-dirs	don't send implied dirs with —relative
b	backup	make backups
	backup-dir	make backups into hierarchy based in DIR
	suffix	backup suffix (default ~)
u	update	new files are updated
	inplace	update destination files by in-place copy
d	dirs	transfer directories without recursing
l	links	copy symlinks as symlinks
L	copy-links	transform symlink into referent file/dir
	copy-unsafe-links	only “unsafe” symlinks are transformed
	safe-links	ignore symlinks that point outside the tree
k	copy-dirlinks	transform symlink to dir into referent dir
K	keep-dirlinks	treat symlinked dir on receiver as dir
p	perms	preserve permissions
E	executability	preserve executability
	chmod	affect file and/or directory permissions
o	owner	preserve owner
g	group	preserve group

Bytix Archaea tools Command Reference

	devices	preserve device files
	specials	preserve special files
D		specify device files and special files
t	times	preserve modification times
O	omit-dir-times	omit directories from —times
J	omit-link-times	omit symlinks from —times
	super	receiver attempts super-user activities
	sparse	turn sequences of nulls into sparse blocks
n	dry-run	perform a trial run with no changes made
	auto-rerun	automatically rerun
W	whole-file	copy files whole
	one-file-system	copy over one file system
	existing	skip creating new files on receiver
	ignore-existing	skip updating files that exist on receiver
	del	an alias for —delete-during
	delete	delete extraneous files from dest dirs
	delete-before	receiver deletes before xfer, not during
	delete-during	receiver deletes during the transfer
	delete-delay	find deletions during, delete aft
	delete-after	receiver deletes after transfer, not during
	delete-excluded	delete excluded files from dest dirs
	force	force deletion of dirs even if not empty
	max-delete	don't delete more than NUM files
	max-size	don't transfer any file larger than SIZE
	min-size	don't transfer any file smaller than SIZE
	partial	keep partially transferred files
	partial-dir	put a partially transferred file into DIR
m	prune-empty-dirs	prune empty directory chains from file-list
	numeric-ids	don't map uid/gid values by user/group name
	usermap	custom username mapping
	groupmap	custom groupname mapping
	chown	simple username/groupname mapping
I	ignore-times	don't skip files that match size and time

Bytix Archaea tools Command Reference

	size-only	skip files that match in size
@	modify-window	set the accuracy for mod-time comparisons
T	temp-dir	create temporary files in directory DIR
z	compress	compress file data during the transfer
	compress-level	explicitly set compression level
	hcp-exclude	exclude HCP files from transfer
f	filter	add a file-filtering
	exclude	add a rule to exclude files
	exclude-from	read exclude patterns from a file
	include	add a rule to include files
	include-from	read include patterns from a file
	files-from	read a list of source-file names from a file
	stats	give some file-transfer stats
h	human-readable	output numbers in a human-readable format
	progress	show progress during transfer
P		specify partial and progress settings
i	itemize-changes	output a change-summary for all updates
	out-format	output updates using the specified format
	log-file	specify a file where to log
	bwlimit	limit socket I/O bandwidth
	stop-at	Stop rsync at the specified point in time
	stop-after	Stop rsync after the specified time have elapsed
	hpf	force HpFP protocol to be used
	wss	use the WebSocket protocol (SSL/TLS)
	fio-extension	use file I/O extension (beta, Linux)
	fio-direct	use Direct I/O (beta, Linux)
	fio-async-linux	use Linux asynchronous I/O (beta, Linux)
V	version	show the version
	config-test	show the configuration and run results
h	help	show command line help
	user	username
	password	password
	config-file	configuration file

	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	HCP diagnostic log file
	hcp-stat-log-file	HCP stats log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	fio-direct-align	alignment size on Direct I/O
	fio-direct-align-local	alignment size on source site
	fio-direct-align-remote	alignment size on destination site
	fio-direct-malloc	how to malloc with alignment
	fio-direct-reuse-aligned	reuse allocated memory with alignment
	fio-direct-threshold	threshold of files for Direct I/O
	fio-async-max-events	maximum events of asynchronous I/O
	fio-async-max-get-events	maximum events to get on asynchronous I/O
	fio-async-get-events-timeo	timeout on getting events on asynchronous I/O
	fio-fallocate	how making pre-allocation of storage
	fio-fallocate-unit	unit size of the pre-allocation
	fio-no-extension-	suppress file I/O extension on source site

	local	
	fio-no-extension-remote	suppress file I/O extension on destination site
	fio-extension-always	force file I/O extension for all files
	hcp-out	specify the file to output execution results
	investigation	investigation mode
	multi-run	multiple-run mode
	dry-run-keep-read	no disk I/O, but keep reading
	dry-run-keep-write	no disk I/O, but keep writing
	dry-run-keep-memalign	no disk I/O and Direct I/O, but keep malloc with alignment
	no-agent	don't use agent
	ident-select	select identity
	mcd	set the number of maximum connections per session
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --fio-extension, --fio-direct, --fio-async-linux, --sparse, --user, --password, --config-file, --config-option, --show-config-option, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --hcp-stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --fio-direct-align, --fio-direct-align-local, --fio-direct-align-remote, --fio-direct-malloc, --fio-direct-reuse-aligned, --fio-direct-threshold, --fio-async-max-events, --fio-async-max-get-events, --fio-async-get-events-timeo, --fio-fallocate, --fio-fallocate-unit, --fio-no-extension-local, --fio-no-extension-remote, --fio-extension-always, --hcp-out, --multi-run, --dry-run-keep-read, --dry-run-keep-write, --dry-run-keep-memalign, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat, --mcd

—hcp-stat-log-file, —dry-run-keep-read, —dry-run-keep-write and —dry-run-keep-memalign are corresponding to —stat-log-file, —no-diskio-keep-read, —no-diskio-keep-write and —no-diskio-keep-memalign of the hcp command respectively.

1.4.1 v, verbose

```
=====
Supported OS : Linux / Windows / Mac
Format : -v | --verbose
=====
```

The redundancy level of the application outputs is raised by one step. As it goes up, more detailed and more information is output.

hsync produces the following logs each verbosity.

```
-v   : NAME1, STATS1, DEL1
-vv  : SKIP
-vvv : none
```

DEL1 dose not make logs about sub directories in some cases, e.g. using —delete-excluded.

```
--
Example :
[user@localhost ~]$ hsync -v ...
[user@localhost ~]$ hsync -vv ...
--
```

1.4.2 q, quiet

```
=====
Supported OS : Linux / Windows / Mac
Format : -q | --quiet
=====
```

Suppress non-error message outputs.

```
--
Example :
[user@localhost ~]$ hcp -q ...
--
```

1.4.3 c, checksum

```
=====
Supported OS : Linux / Windows / Mac
Format : -c | --checksum
=====
```

When a checksum doesn't match, it behaves to transmit the file.

--

Example :

```
[user@localhost ~]$ hsync -c ...
```

--

1.4.4 a, archive

```
=====
Supported OS : Linux / Windows / Mac
Format : -a | --archive
=====
```

It behaves the same as -rflptgo. This option is effective to set a directory archive with maintaining the file attribute.

--

Example :

```
[user@localhost ~]$ hsync -a ...
```

--

1.4.5 r, recursive

```
=====
Supported OS : Linux / Windows / Mac
Format : -r | --recursive
=====
```

It recursively searches directories and transmits files.

--

Example :

```
[user@localhost ~]$ hsync -r ...
```

--

1.4.6 R, relative

```
=====
Supported OS : Linux / Windows / Mac
Format : -R | --relative
=====
```

Use relative paths.

--

Example :

```
[user@localhost ~]$ hsync -R ...
```

--

1.4.7 no-implied-dirs

```
=====
Supported OS : Linux / Windows / Mac
```

Format : --no-implied-dirs

When `—relative` is used, this suppresses sending information of intermediate directories of relative paths given from the command line arguments. It results in preventing `hsync` from removing symbolic links on a path corresponding to the intermediate directories on the receiver side due to collision of file types. `—keep-dirlinks` also works for this purpose.

--

Example :

```
[user@localhost ~]$ hsync --no-implied-dirs ...
```

--

1.4.8 b, backup

Supported OS : Linux / Windows / Mac

Format : -b | --backup

In backup, if a file with the same name exists in the destination, the transferring file is renamed.

--

Example :

```
[user@localhost ~]$ hsync -b ...
```

--

1.4.9 backup-dir

Supported OS : Linux / Windows / Mac

Format : --backup-dir=<dir-name>

dir-name

Default : none

Range of Values : path component characters

A directory name to backup is specified.

--

Example :

```
[user@localhost ~]$ hsync --backup-dir=backup_20211013 ...
```

--

1.4.10 suffix

```
=====
Supported OS : Linux / Windows / Mac
Format : --suffix=<suffix-name>
=====
```

The suffix to rename for backup is specified.

```
--
Example :
[user@localhost ~]$ hsync --suffix=.bk ...
--
```

1.4.11 u, update

```
=====
Supported OS : Linux / Windows / Mac
Format : -u | --update
=====
```

It doesn't transfer files that are newer on the destination. In the case of the same update time, when the file size is different, It will be transmitted.

```
--
Example :
[user@localhost ~]$ hsync -u ...
--
```

1.4.12 inplace

```
=====
Supported OS : Linux / Windows / Mac
Format : --inplace
=====
```

It instructs the receiver to write files without temporary files. When transferring a file is aborted, the file is kept as a partial file. Resuming the file will be performed when a digest of the partial file is identical to one of the source file in range from the head to a length of the partial file.

```
--
Example :
[user@localhost ~]$ hsync --inplace ...
--
```

1.4.13 d, dirs

```
=====
Supported OS : Linux / Windows / Mac
```

Format : -d | --dirs

=====

It instructs the source to include all directories that are encountered. Unlike `—recursive`, a directory's contents are not copied, unless the tail end of the directory name is specified with `"."` or `"/"`.

--

Example :

```
[user@localhost ~]$ find from_dir/
from_dir/
from_dir/dir01
from_dir/dir02
from_dir/dir02/file02.txt
from_dir/dir03
from_dir/dir03/dir03_1
from_dir/dir03/dir03_1/file03_1.txt
from_dir/dir03/dir03_1/file03_2.txt
from_dir/file.txt
[user@localhost ~]$ hsync --dirs ... from_dir/ to_dir/
[user@localhost ~]$ find to_dir/
to_dir
to_dir/dir01
to_dir/dir02
to_dir/dir03
to_dir/file.txt
--
```

1.4.14 `l`, links

Supported OS : Linux / Mac

Format : -l | --links

=====

The symbolic link from the source is copied directly to the destination.

If you do not specify any options related to link-copy, such as `—links`, `—copy-links`, etc., symbolic links are not copied to destinations.

--

Example :

```
[user@localhost ~]$ hsync -l ...
```

--

1.4.15 `L`, copy-links

Supported OS : Linux / Mac

Format : -L | --copy-links

It transforms each symlink encountered in the source into the referent item following the symlink chain to the file or directory that it references. And then it copies it to the destination.

If you do not specify any options related to link-copy, such as `—links`, `—copy-links`, etc., symbolic links are not copied to destinations.

--

Example :

```
[user@localhost ~]$ hsync -L ...
```

--

1.4.16 copy-unsafe-links

Supported OS : Linux / Mac

Format : --copy-unsafe-links

“unsafe” symbolic links are first resolved to the referent of symbolic and copied to the destination.

“unsafe” symbolic links are the followings.

- symbolic links pointing outside the copied tree.
- symbolic links pointing to absolute paths.

--

Example :

```
[user@localhost ~]$ hsync --copy-unsafe-links ...
```

--

1.4.17 safe-links

Supported OS : Linux / Mac

Format : --safe-links

This command instructs not to copy “unsafe” symbolic links themselves to the destinations.

“unsafe” symlinks copies are skipped in `—copy-links` or `—copy-unsafe-links` unless any options specify the referents to copy.

--

Example :

```
[user@localhost ~]$ hsync --safe-links ...  
--
```

1.4.18 k, copy-dirlinks

```
=====
Supported OS : Linux / Mac
Format : -k | --copy-dirlinks
=====
```

hsync follows symbolic links at source refer to directories and copy the directories in names of the symbolic links to the destination. This option dose not resolve symbolic links to files.

```
--
Example :
[user@localhost ~]$ hsync --copy-dirlinks ...
--
```

1.4.19 K, keep-dirlinks

```
=====
Supported OS : Linux / Mac
Format : -K | --keep-dirlinks
=====
```

hsync keeps symbolic links pointed to directories on the receiver side without deleting the links. And it transfer files recursively when -r option is specified as if the kept links are directories.

When this option is not set and a directory whose name is identical to the name of the link exists on the sender side, hsync determines they are conflicted resources and delete the link to replace by the directory. This option suppresses this behavior.

```
--
Example :
[user@localhost ~]$ hsync --keep-dirlinks ...
--
```

1.4.20 p, perms

```
=====
Supported OS : Linux / Mac
Format : -p | --perms
=====
```

The source permissions are maintained at the destination when copying.

```
--
Example :
```

```
[user@localhost ~]$ hsync -p ...  
--
```

1.4.21 E, executability

```
=====
Supported OS : Linux / Mac
Format : -E | --executability
=====
```

Execute permissions in the destination are set by judging the file executability in the source.

When a file has an execution attribute of any of owner, group, or other, it is judged to be executable. In the case that the execution attribute is different between the source and destination, the file permission in the destination is modified as follows.

- To make a file non-executable, all execution attribute 'x' is turned off.
- To make a file executable, the execution attribute 'x' of the field where a read attribute 'r' is set, is turned on.

```
--
Example :
[user@localhost ~]$ hsync -E ...
--
```

1.4.22 chmod

```
=====
Supported OS : Linux / Mac
Format : --chmod=<modifier>[,<modifier>...]
-----
modifier
Default : none
Range of Values : permission modifiers (based on the chmod command)
=====
```

This option applies the specified permission to the file.

Permission modifiers follow the format of the chmod command, whose extension format is below.

```
https://download.samba.org/pub/rsync/rsync.1
--chmod=CHMOD
```

```
--
Example :
[user@localhost ~]$ hsync --chmod=Dg+s,ug+w,Fo-w,+X ...
[user@localhost ~]$ hsync --chmod=D2775,F664 ...
--
```

1.4.23 o, owner

```
=====
Supported OS : Linux / Mac
Format : -o | --owner
=====
```

This option maintains the owner of the source file when copying.

When `—numeric-ids` is not set, UID is set by resolving from the username of the owner attribute in the source files on the destination host. In the case of UID can't be resolved, such as no user, etc., UID is set the same value as the source file.

```
--
Example :
[user@localhost ~]$ hsync -o ...
--
```

1.4.24 g, group

```
=====
Supported OS : Linux / Mac
Format : -g | --group
=====
```

This option maintains the group of the source file when copying.

When `—numeric-ids` is not set, GID is set by resolving from the groupname in the group attribute on the source files on the destination host. If GID can't be resolved, such as no group, etc., GID is set at the same value as the source file.

```
--
Example :
[user@localhost ~]$ hsync -g ...
--
```

1.4.25 devices

```
=====
Supported OS : Linux / Mac
Format : --devices
=====
```

This tells hsync to copy device files. When this option is not set, device files will be skipped.

```
--
Example :
[user@localhost ~]$ hsync --devices ...
--
```

1.4.26 specials

```
=====
Supported OS : Linux / Mac
Format : --specials
=====
```

This tells hsync to copy special files (FIFO and sockets). When this option is not set, special files will be skipped.

```
--
Example :
[user@localhost ~]$ hsync --specials ...
--
```

1.4.27 D

```
=====
Supported OS : Linux / Mac
Format : -D
=====
```

This tells hsync to use `—devices` and `—specials`.

```
--
Example :
[user@localhost ~]$ hsync -D ...
--
```

1.4.28 t, times

```
=====
Supported OS : Linux / Windows / Mac
Format : -t | --times
=====
```

This option maintains the modification time of the source file.

```
--
Example :
[user@localhost ~]$ hsync -t ...
--
```

1.4.29 O, omit-dir-times

```
=====
Supported OS : Linux / Windows / Mac
Format : -O | --omit-dir-times
=====
```

This option doesn't maintain the modification times of the directory when copying.

```
--  
Example :  
[user@localhost ~]$ hsync -O ...  
--
```

1.4.30 J, omit-link-times

```
=====
```

Supported OS : Linux / Windows / Mac
Format : -J | --omit-link-times

```
=====
```

This option doesn't maintain the modification times of the symbolic link when copying.

```
--  
Example :  
[user@localhost ~]$ hsync -J ...  
--
```

1.4.31 super

```
=====
```

Supported OS : Linux / Mac
Format : --super

```
=====
```

This tells hsync to perform some operations which requires privileges like the following operations. When this option is not set, hsync will determine to perform or not to subject to user's access rights on the receiver side.

- Change owner of files
- Change group of files
- Copy device files

—no-super also tells hsync not to perform them regardless of user's access rights.

```
--  
Example :  
[user@localhost ~]$ hsync --super ...  
--
```

1.4.32 dry-run

```
=====
```

Supported OS : Linux / Windows / Mac
Format : --dry-run

```
=====
```

This option makes a trial copy without practically operating the file.


```
--  
Example :  
[user@localhost ~]$ hsync --dry-run ...  
--
```

1.4.33 auto-rerun

```
=====
```

Supported OS : Linux / Windows / Mac
Format : --auto-rerun

```
=====
```

It automatically restarts synchronization when transmission stops due to network errors. However, in the case that a user stops copying by Ctrl+C, it doesn't restart it at that time.

If the number of trials to restart is unlimited and you uses the option of `—ignore-times`, the starting synchronization will be stopped without running.

It is recommended to use private keys that are not encrypted by passphrases for this purpose. If you need the passphrases, hcp make a cache on the memory of that passphrase to prevent interactive prompts from being shown for re-authentication.

1.4.34 W, whole-file

```
=====
```

Supported OS : Linux / Windows / Mac
Format : -W | --whole-file

```
=====
```

On resuming a file, this option tells hsync to copy the total of the file from the head, but not from a resuming position.

```
--  
Example :  
[user@localhost ~]$ hsync -W ...  
--
```

1.4.35 one-file-system

```
=====
```

Supported OS : Linux / Mac
Format : --one-file-system

```
=====
```

This option tells hsync to skip files residing on other file systems. Twice or more specification indicates hsync run without making directories on the boundaries.

```
--  
Example :
```

```
// Boundary directories that are residing on other file systems will be made.
[user@localhost ~]$ hsync --one-file-system ...
// Such directories will not be made.
[user@localhost ~]$ hsync --one-file-system --one-file-system ...
--
```

1.4.36 existing

```
=====
Supported OS : Linux / Windows / Mac
Format : --existing
=====
```

This option copies files existing on the destination but skips copying the files which do not exist yet on the destination.

```
--
Example :
[user@localhost ~]$ hsync --existing ...
--
```

1.4.37 ignore-existing

```
=====
Supported OS : Linux / Windows / Mac
Format : --ignore-existing
=====
```

This option copies files which do not exist yet on the destination but skips updating the files existing on the destination.

```
--
Example :
[user@localhost ~]$ hsync --ignore-existing ...
--
```

1.4.38 del

```
=====
Supported OS : Linux / Windows / Mac
Format : --del
=====
```

This option is an alias for `—delete-during`.

```
--
Example :
[user@localhost ~]$ hsync --del ...
--
```

1.4.39 delete

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete
=====
```

This option deletes files and directories in the destination that don't exist in the source.

```
--
Example :
[user@localhost ~]$ hsync --delete ...
--
```

1.4.40 delete-before

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete-before
=====
```

This option requests file deletions be executed before the transfer.

```
--
Example :
[user@localhost ~]$ hsync --delete-before ...
--
```

1.4.41 delete-during

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete-during
=====
```

This option requests file deletions be executed during the transfer.

This is the default —delete operation mode.

```
--
Example :
[user@localhost ~]$ hsync --delete-during ...
--
```

1.4.42 delete-delay

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete-delay
=====
```

This option requests file deletions be executed after the transfer, but determining its deletions on transfer.

```
--  
Example :  
[user@localhost ~]$ hsync --delete-delay ...  
--
```

1.4.43 delete-after

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete-after
=====
```

This option requests file deletions be executed after the transfer.

```
--  
Example :  
[user@localhost ~]$ hsync --delete-after ...  
--
```

1.4.44 delete-excluded

```
=====
Supported OS : Linux / Windows / Mac
Format : --delete-excluded
=====
```

This option tells hsync to remove files which are excluded from transfer.

```
--  
Example :  
[user@localhost ~]$ hsync --delete-excluded ...  
--
```

1.4.45 force

```
=====
Supported OS : Linux / Windows / Mac
Format : --force
=====
```

This option requests to delete non-empty directories.

This option is used to delete a directory, even though it is not empty, in the case that the source is a file or symbolic link and the destination directory is supposed to be deleted or overwritten. If this option is not set in the above condition, the destination directory is not deleted, and the source file transfer is skipped.

```
--  
Example :  
[user@localhost ~]$ hsync --force ...  
--
```

1.4.46 max-delete

```
=====
Supported OS : Linux / Windows / Mac
Format : --max-delete=<max-num>
-----
max-num
Default : none
Range of Values : -1, 0 - maximum value of signed integer
=====
```

The max number of files and directories to be deleted is set.

The max number is set at max-num. When 0 or -1, deleting is not operated.

```
--
Example :
[user@localhost ~]$ hsync --max-delete=100 ...
--
```

1.4.47 max-size

```
=====
Supported OS : Linux / Windows / Mac
Format : --max-size=<size>
-----
size
Default : none
Range of Values : numeric value, numeric string with unit
=====
```

The maximum size of the file to be transferred is set.

Numeric value or numeric string including the units (B, K, M, G, T, P) can be set as the maximum file size. Please find the format of the numeric string with the units on the following website.

<https://download.samba.org/pub/rsync/rsync.1>
--max-size=SIZE

The following setting items that limit the size of the file used in the hcp commands are ignored in the hsync ones.

- MaxReceiveFileSize
- MaxSendFileSize

--

Example :

```
[user@localhost ~]$ hsync --max-size=1000 ...
```

```
[user@localhost ~]$ hsync --max-size=1.5mb-1 ...
```

--

1.4.48 min-size

Supported OS : Linux / Windows / Mac

Format : --min-size=<size>

size

Default : none

Range of Values : numeric value, numeric string with unit

The minimum size of the file to be transferred is set.

Numeric value or numeric string including the units (B, K, M, G, T, P) can be set as the minimum file size. It supports the same format as `--max-size`.

--

Example :

```
[user@localhost ~]$ hsync --min-size=1000 ...
```

```
[user@localhost ~]$ hsync --min-size=1.5mb-1 ...
```

--

1.4.49 partial

Supported OS : Linux / Windows / Mac

Format : --partial

This tells hsync to keep files on the receiver side which are aborted on transfer.

--

Example :

```
[user@localhost ~]$ hsync --partial ...
```

--

1.4.50 partial-dir

Supported OS : Linux / Windows / Mac

Format : --partial-dir=<dir_path>

dir_path

Default : none

Range of Values : path string of file system

=====

This option specifies a directory path to keep files which are aborted on transfer. When the path is a relative one, a directory to keep an aborted file will be created at a directory where hsync writes the file on the receiver side.

If hsync detects an aborted file on the directory, it tries to resume the file. Only using `--partial` does not make this resuming operation.

--

Example1 :

```
[user@localhost ~]$ hsync --partial-dir=_part_dir_ ...
```

Example2 :

```
[user@localhost ~]$ hsync --partial-dir=/home/user/_part_dir_ ...
```

--

1.4.51 m, prune-empty-dirs

=====

Supported OS : Linux / Windows / Mac

Format : `-m` | `--prune-empty-dirs`

=====

This option instructs not to transfer empty directories.

It is useful to avoid unnecessary filter-rule checking by `include/exclude/filter`.

--

Example :

```
[user@localhost ~]$ hsync -m ...
```

--

1.4.52 numeric-ids

=====

Supported OS : Linux / Mac

Format : `--numeric-ids`

=====

This option instructs to maintain the file ownership and group at the destination with UID/GID in the source file.

--

Example :

```
[user@localhost ~]$ hsync --numeric-ids ...
```

--

1.4.53 usermap

```
=====
Supported OS : Linux / Mac
Format : --usermap=<mapping>[,<mapping>...]
-----
mapping
Default : none
Range of Values : string describing user mapping by its names and UIDs
=====
```

When maintaining the sender's ownership in a destination file by the `—owner` option, it instructs to do that after specified user mapping.

A string described user mapping is set in mapping. The source can be a username or UID value. The destination can be a username or UID value as well. Please refer to the following web site regarding the format.

<https://download.samba.org/pub/rsync/rsync.1>
`--usermap=STRING, --groupmap=STRING`

```
--
Example :
[user@localhost ~]$ hsync --usermap=0-99:nobody,wayne:admin,*:normal ...
--
```

1.4.54 groupmap

```
=====
Supported OS : Linux / Mac
Format : --groupmap=<mapping>[,<mapping>...]
-----
mapping
Default : none
Range of Values : string describing group mapping by its names and GIDs
=====
```

When maintaining the sender's group in a destination file by the `—group` option, it instructs to do that after specified group mapping.

A string described group mapping is set in mapping. The source can be a group name or GID value. The destination can be a group name or GID value as well. Please refer to the following web site regarding the format.

<https://download.samba.org/pub/rsync/rsync.1>
`--usermap=STRING, --groupmap=STRING`

```
--
Example :
```



```
[user@localhost ~]$ hsync --groupmap=usr:1,1:usr ...  
--
```

1.4.55 chown

```
=====
Supported OS : Linux / Mac
Format : --chown=<user>[:<group>]
-----
user
Default : none
Range of Values : user name
-----
group
Default : none
Range of Values : group name
=====
```

It instructs to apply the specified username and group name to the owner and group.

This option adopts the `—usermap` or `—groupmap` option. For example, the following two commands result in the same.

```
[user@localhost ~]$ hsync --chown=foo:bar ...
[user@localhost ~]$ hsync --usermap=*:foo --groupmap=*:bar ...
```

1.4.56 I, ignore-times

```
=====
Supported OS : Linux / Windows / Mac
Format : -I | --ignore-times
=====
```

It instructs to copy file even if its size and update time are the same between source and destination.

```
--
Example :
[user@localhost ~]$ hsync -I ...
--
```

1.4.57 size-only

```
=====
Supported OS : Linux / Windows / Mac
Format : --size-only
=====
```

It instructs to copy files as long as their size are different between source and destination. The update time is ignored. Even when the update time is the same, the file is copied.

```
--
Example :
[user@localhost ~]$ hsync --size-only ...
--
```

1.4.58 @, modify-window

```
=====
Supported OS : Linux / Windows / Mac
Format : -@<mod_win_time> | --modify-window=<mod_win_time>
-----
mod_win_time
Default : 0
Range of Values : modification window time (in secs)
=====
```

This option specifies a modification window time that indicates a margin to compare timestamps of files for determining a file is newer, older or equal to another one. When 0 is set, hsync determines two files are same in time if timestamps of them completely matches in seconds. When a value over 0 is set, it dose if the difference of their timestamps is in range of the value.

Any negative value is not supported (in rsync, it is supposed to specify a nanoseconds).

```
--
Example :
[user@localhost ~]$ hsync --modify-window=3 ...
// Files whose difference of timestamps is under 3 seconds or equals to i
t will be decided as same files in time.
--
```

1.4.59 T, temp-dir

```
=====
Supported OS : Linux / Windows / Mac
Format : -T <dir_path> | --temp-dir=<dir_path>
-----
dir_path
default : none
Range of Values : path string of file system
=====
```

This option specifies a directory path to make temporary files. When the path is a relative one, an existing directory on the destination directory given from the command line will be used. When this option is not set, a temporary file of each file will be created at a directory where hsync writes the file on the receiver side.

Transfer of files results in failure if the directory indicated by this option dose not exist on the receiver side.

--

Example1 :

```
[user@localhost ~]$ hsync --temp-dir=_temp_dir_ ... /path/to/src 192.168.1.100:/path/to/dst
```

// /path/to/dst/_temp_dir_ is the temporary directory of this transfer.

Example2 :

```
[user@localhost ~]$ hsync --temp-dir=/home/user/_temp_dir_ ...
```

--

1.4.60 z, compress

```
=====
Supported OS : Linux / Windows / Mac
Format : -z | --compress
=====
```

It instructs to compress files data to send.

This command compresses all messages communicating with a server, such as messages including file data, control messages to request sending files, etc.

--

Example :

```
[user@localhost ~]$ hsync -z ...
```

--

1.4.61 compress-level

```
=====
Supported OS : Linux / Windows / Mac
Format : --compress-level=<level>
-----
level
Default : 5
Range of Values : 0 - 9
=====
```

It set the compress level.

--

Example :

```
[user@localhost ~]$ hsync --compress-level=5 ...
```

--

1.4.62 hcp-exclude

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-exclude
=====
```

This option tells hsync to exclude the following files from its file transfer that will be generated by hsync in its running.

- Linux/macOS : .hcp.out, .hcp.in, .hcp.diag, .hcp.statistics.*
- Windows : _hcp.out, _hcp.in, _hcp.diag, _hcp.statistics.*

You can also use `—filter` options for this purpose.

This option actually uses exclude filters described below. When you specify this option in one time, hsync will register exclude filters for the running (client) platform that reject files which are generated on that platform by hsync. When specifying twice, hsync will register other exclude filters that reject files which are not generate on that platform.

```
--  
Example :  
[user@localhost ~]$ hsync --hcp-exclude ...  
  
[user@localhost ~]$ hsync --filter="-H" ...  
--
```

1.4.63 f, filter

```
=====
Supported OS : Linux / Windows / Mac
Format : -f <filter-desc> | --filter=<filter-desc>
-----
filter-desc
Default : none
Range of Values : filter strings
=====
```

It adds the filter to select a file. The filters (including `—exclude`, `—exclude-from`, `—include`, `—include-from` as will be described later.) are applied in the order of the description. Please refer to the following description on its format and rules, etc.

```
https://download.samba.org/pub/rsync/rsync.1
FILTER RULES
INCLUDE/EXCLUDE PATTERN RULES
MERGE-FILE FILTER RULES
LIST-CLEARING FILTER RULE
ANCHORING INCLUDE/EXCLUDE PATTERNS
PER-DIRECTORY RULES AND DELETE
```

hsync provides a unique parameter of “H” for exclude/include modifiers (see the `—hcp-exclude` option for more detail).

The following functions have not yet been implemented on this version.

```
- Merge filter(merge, dir-merge)
- "/", "C", "S", "r", "p", "x" among exclude/include modifiers.

--
Example :
// search for any .c files in all directories and copy them.
[user@localhost ~]$ hsync --filter="+ */" --filter="+ *.c" --filter="- *"
...
// the same result as the above command
[user@localhost ~]$ hsync --include="*/" --filter="+ *.c" --exclude="*"
...
--
```

1.4.64 exclude

```
=====
Supported OS : Linux / Windows / Mac
Format : --exclude=<exclude-desc>
-----
exclude-desc
Default : none
Range of Values : excluded filter strings
=====
```

It adds excluded filters. Please refer to the following description on its format and rules, etc.

<https://download.samba.org/pub/rsync/rsync.1>
FILTER RULES
INCLUDE/EXCLUDE PATTERN RULES

In this option, modifiers for the exclude rule described earlier cannot be described. When "+" is put at the beginning, the include rule is adopted. When "!" is put at the beginning, the clear rule is adopted.

```
--
Example :
[user@localhost ~]$ hsync --exclude="*.c" ...
--
```

1.4.65 exclude-from

```
=====
Supported OS : Linux / Windows / Mac
Format : --exclude-from=<file>
-----
file
Default : none
```

Range of Values : path string of file to read excluded rules

=====

It adds a file to read excluded rules. Please refer to the following description on its format and rules, etc.

<https://download.samba.org/pub/rsync/rsync.1>

FILTER RULES

INCLUDE/EXCLUDE PATTERN RULES

When another filter rules are specified before and after, the rule read from a file is put between them.

--

Example :

```
[user@localhost ~]$ cat .exclude-rule
```

```
*
```

```
[user@localhost ~]$ hsync --include="*/" --include="*.c" --exclude-from=".  
exclude-rule" ...
```

--

1.4.66 include

=====

Supported OS : Linux / Windows / Mac

Format : --include=<include-desc>

include-desc

Default : none

Range of Values : included filter strings

=====

It adds included filters. Please refer to the following description on its format and rules, etc.

<https://download.samba.org/pub/rsync/rsync.1>

FILTER RULES

INCLUDE/EXCLUDE PATTERN RULES

In this option, modifiers for the include rule described earlier cannot be described. When “-” is put at the beginning, the exclude rule is adopted. When “!” is put at the beginning, the clear rule is adopted.

--

Example :

```
[user@localhost ~]$ hsync --include="*.c" ...
```

--

1.4.67 include-from

```
=====
Supported OS : Linux / Windows / Mac
Format : --include-from=<file>
-----
file
Default : none
Range of Values : path string of file to read included rules
=====
```

It adds a file to read included rules. Please refer to the following description on its format and rules, etc.

<https://download.samba.org/pub/rsync/rsync.1>

FILTER RULES

INCLUDE/EXCLUDE PATTERN RULES

When another filter rules are specified before and after, the rule read from a file is put between them.

```
--
Example :
[user@localhost ~]$ cat .include-rule
*/
*.c
[user@localhost ~]$ hsync --include-from=".include-rule" --exclude="*" ...
--
```

1.4.68 files-from

```
=====
Supported OS : Linux / Windows / Mac
Format : --files-from=<file>
-----
file
Default : none
Range of Values : path string of file to read a file list
=====
```

This tells hsync to read a list of files from the specified file.

```
--
Example :
[user@localhost ~]$ hsync --files-from=source.file.list ...
--
```

1.4.69 stats

```
=====
Supported OS : Linux / Windows / Mac
```

Format : --stats

=====

This tells hsync to output statistics data of file transfer.

When the verbosity by -v option is 0 or 1, logs of STATS2 will be output.

--

Example :

[user@localhost ~]\$ hsync --stats ...

--

1.4.70 h, human-readable

=====

Supported OS : Linux / Windows / Mac

Format : -h | --human-readable

=====

This tells hsync to output numbers in a human-readable format.

--

Example :

[user@localhost ~]\$ hsync --human-readable ...

--

1.4.71 progress

=====

Supported OS : Linux / Windows / Mac

Format : --progress

=====

This tells hsync to output progress of file transfer. However, printing a ratio of transferred bytes is not supported.

When NAME1 and PROGRESS1 by —info options are set, the same output will be produced.

--

Example :

[user@localhost ~]\$ hsync --progress ...

--

1.4.72 P

=====

Supported OS : Linux / Windows / Mac

Format : -P

=====

This tells hsync to enable `—partial` and `—progress`.

--

Example :

```
[user@localhost ~]$ hsync -P ...
```

--

1.4.73 `i`, `itemize-changes`

```
=====
Supported OS : Linux / Windows / Mac
Format : -i | --itemize-changes
=====
```

This tells hsync to print a summary of changing files. When `—out-format="%i %n%L"` is set, the same output will be produced.

For the field of 'Y', "h", "." and "*" will not be produced.

For the field of 'u(n|b)', 'a' and 'x', only ".", "+" and "?" will be produced due to no support for `—atime`, etc.

--

Example :

```
[user@localhost ~]$ hsync --itemize-changes ...
```

--

1.4.74 `out-format`

```
=====
Supported OS : Linux / Windows / Mac
Format : --out-format=<format>
-----
Format
Default : %n%L
Range of Values : format specification string
=====
```

This tells a format specification string to hsync for logging updates of files. It supports the following items.

- %b Actual transfered size
- %B Permission
- %C Checksum (Hex notation)
- %G GID
- %i `—itemize-changes`

- %L Symbolik link target name
- %l File size
- %M Modification date and time
- %n File name
- %o Operation name (send or recv)
- %p Process ID
- %t Current date and time
- &u User name
- %U UID

--

Example :

```
[user@localhost ~]$ hsync --out-format="%i %l %n%L" ...
```

--

1.4.75 log-file

Supported OS : Linux / Windows / Mac

Format : --log-file=<file>

file

Default : none

Range of Values : path string of file system

=====

This tells hsync to output progress logs of file transfer to a log file. This output will be performed in addition to output to the standard output.

--

Example :

```
[user@localhost ~]$ hsync --log-file=hsync.log --exclude="hsync.log" ...
```

--

1.4.76 bwlimit

Supported OS : Linux / Windows / Mac

Format : --bwlimit=<bw-desc>

bw-desc

Default : none

Range of Values : numeric value (byte), throughput string with unit (byt

e)

=====

The maximum bandwidth for sending and receiving is set.

bw-desc is numeric value or string for specifying throughput with B, K, M, G, T, or P.
The unit is byte. The format is the same as `—max-size`.

How to limit the bandwidth by this option is the same method as
`MaxSendRate/MaxReceiveRate` in the settings.

--

Example :

```
[user@localhost ~]$ hsync --bwlimit=1000000 ...
```

```
[user@localhost ~]$ hsync --bwlimit=1mb ...
```

--

1.4.77 stop-at

=====

Supported OS : Linux / Windows / Mac

Format : `--stop-at=<timestamp-desc>`

timestamp-desc

Default : none

Range of Values : y-m-dTh:m

=====

This specifies an expire of file transfer running by a date and time.

If the transfer continues at the date and time, hsync will abort the transfer.

--

Example :

```
[user@localhost ~]$ hsync --stop-at=2022-1-1
```

```
[user@localhost ~]$ hsync --stop-at=1-1 // until 1/1 00:00 the next year
```

```
[user@localhost ~]$ hsync --stop-at=30 // until 00:00 the next 30th
```

```
[user@localhost ~]$ hsync --stop-at=12:00 // until the next 12:00 (of tod  
ay or tomorrow)
```

```
[user@localhost ~]$ hsync --stop-at=:30 // until the next xx:30
```

--

1.4.78 stop-after

=====

Supported OS : Linux / Windows / Mac

Format : `--stop-after=<mins-desc>`

mins-desc

Default : -1

Bytix Archaea tools Command Reference

Range of Values : -1, 0 - maximum value of signed integer (minute)

The maximum execution time is set.

The maximum execution time is specified in the minute unit. When -1 is set, the limitation is not set.

When the execution time passes but copying hasn't been completed, copying is suspended.

--

Example :

```
[user@localhost ~]$ hsync --stop-after=30 ...
```

--

1.4.79 V, version

Supported OS : Linux / Windows / Mac

Format : -V | --version

The hsync command version is shown.

--

Example :

```
[user@localhost ~]$ hsync -V
```

```
hsync client (hsync) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 W  
S 4.2.0-2)
```

--

1.4.80 config-test

Supported OS : Linux / Windows / Mac

Format : --config-test

The hsync command parameters and configuration parameters are shown.

--

Example :

```
[user@localhost ~]$ hsync --config-test
```

...

```
-- [Sources] -----
```

```
-- [Destination] -----
```

Bytix Archaea tools Command Reference

```
-- [Command Options] -----  
---  
verbose      : -  
info         : -  
quiet        : disable  
checksum     : disable  
archive      : disable  
recursive    : disable  
relative     : disable  
no-implied-dirs: disable  
backup       : disable  
backup-dir   : -  
suffix       : -  
update       : disable  
inplace      : disable  
dirs         : disable  
links        : disable  
copy-links   : disable  
copy-unsafe-links : disable  
safe-links   : disable  
copy-dirlinks : disable  
keep-dirlinks : disable  
perms        : disable  
executability : disable  
chmod        : -  
owner        : disable  
group        : disable  
devices      : disable  
specials     : disable  
-D           : disable  
times        : disable  
omit-dir-times : disable  
omit-link-times: disable  
super        : disable  
no-super     : disable  
dry-run      : disable  
auto-rerun   : disable  
whole-file   : disable  
one-file-system: disable  
existing      : disable  
ignore-existing: disable  
delete       : disable  
delete-before : disable  
delete-during : disable  
delete-delay  : disable  
delete-after  : disable  
delete-excluded: disable
```

Bytix Archaea tools Command Reference

```
force          : disable
max-delete     : -
max-size       : -
min-size       : -
partial        : disable
partial-dir    : -
prune-empty-dirs : disable
numeric-ids    : disable
usermap        : -
groupmap       : -
chown          : -
ignore-times   : disable
size-only      : disable
modify-window  : - [0]
temp-dir       : -
compress       : disable
compress-level : - [5]
hcp-exclude    : disable
filter         : -
exclude        : -
exclude-from   : -
include        : -
include-from   : -
files-from     : -
stats          : disable
human-readable : disable
progress       : disable
-P             : disable
itemize-changes : disable
out-format     : - [%n%L]
log-file       : -
bwlimit        : -
stop-at        : -
stop-after     : - [-1]
user           : -
password       : -
version        : disable
help           : disable
mcd            : -
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
```

```

StrictHostKeyChecking      : ask
IdentityFile              : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate    : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER                      : user
LOGNAME                   : user
HCP_PASSWORD             :
HCP_WS_PROXY             :
-----
---

Please type '--config-test --config-test ...' for more details.
--

```

1.4.81 h, help

```

=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====

```

The help information on the hsync commands is shown.

When the abbreviation is specified, this option works as long as the destination and source paths are not specified.

```

--
Example :
[user@localhost ~]$ hsync -h
--

```

1.5 hrm

```

Usage: hrm [OPTION]... [USER@]HOST:[PORT:]FILE [:FILE]...
      or: hrm [OPTION]... --host=HOST [--port=PORT] [--user=USER] FILE...

```

The hrm command deletes the files on the remote (server,hcpd server) computer.

abbreviation	option	outline
f	force	delete the file without showing the confirmation

Bytix Archaea tools Command Reference

		message.
R	recursive	delete the file recursively
d	dir	delete the empty directory.
i		show the confirmation message at each deletion.
I		show the confirmation message just once at the first deletion.
n	no-diskio	measure the network I/O performance of communication protocol without disk I/O operations.
	hpfp	use the HpFP protocol
	wss	use the WebSocket protocol (SSL/TLS)
V	version	display the vresion.
	config-test	display the loaded outcome of input parameters and configuration file
h	help	the display command line help
	user	user name
	password	password
	host	remote host
	port	remote port
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol

	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investigation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	select identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.5.1 f, force

```
=====
Supported OS : Linux / Windows / Mac
Format : -f | --force
=====
```

Files are deleted without confirmations, even if necessary due to the access authorization and so on.

```
--
Example :
[user@localhost ~]$ hrm -f ...
--
```

1.5.2 R, recursive

```
=====
Supported OS : Linux / Windows / Mac
Format : -R | --recursive
=====
```

Files are deleted recursively.

```
--  
Example :  
[user@localhost ~]$ hrm -R ...  
--
```

1.5.3 d, dir

```
=====
Supported OS : Linux / Windows / Mac
Format : -d | --dir
=====
```

Even empty directories are deleted.

```
--  
Example :  
[user@localhost ~]$ hrm -d ...  
--
```

1.5.4 i

```
=====
Supported OS : Linux / Windows / Mac
Format : -i
=====
```

The confirmation message is shown at each deletion.

```
--  
Example :  
[user@localhost ~]$ hrm -i ...  
--
```

1.5.5 I

```
=====
Supported OS : Linux / Windows / Mac
Format : -I
=====
```

The confirmation message is not shown after showing it at the first deletion.

```
--  
Example :  
[user@localhost ~]$ hrm -I ...  
--
```

1.5.6 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

Show the hrm command version.

```
--
Example :
[user@localhost ~]$ hrm -V
hrm client (hrm) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS 4.
2.0-2)
--
```

1.5.7 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

Display the input parameters for the hrm command and the configurations.

```
--
Example :
[user@localhost ~]$ hrm --config-test
...

-- [Targets] -----
---
-- [Command Options] -----
---
force          : disable
recursive      : disable
dir            : disable
-i (prompt every) : disable
-I (prompt once) : disable
no-diskio      : disable
host           : -
port           : -
user           : -
password       : -
version        : disable
help           : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication          : yes
```

Bytix Archaea tools Command Reference

```
WinLogonUserAuthentication      : yes
PAMAuthentication              : yes
LocalPasswordAuthentication    : yes
NumberOfPasswordPrompts       : 3
CompressLevel                  : -1
StrictHostKeyChecking          : ask
IdentityFile                   : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.ssh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519 ]
MaxReceiveRate                 : 100000000000
MaxSendRate                    : 100000000000
MaxConnectionReceiveRate       : 100000000000
MaxConnectionSendRate          : 100000000000
TransportTimeout               : 180 sec
AcceptableCryptMethod          : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod         : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER                           : user
LOGNAME                        : user
HCP_PASSWORD                   :
HCP_WS_PROXY                   :
-----
---

Please type '--config-test --config-test ...' for more details.
--
```

1.5.8 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The help for the hrm commands are shown.

```
--
Example :
[user@localhost ~]$ hrm -h
--
```

1.5.9 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
remote-host
```

Bytix Archaea tools Command Reference

Default : none
Range of Values : IP address or host name
=====

The destination remote host is specified, which is applied to the path for the deletion target. With this parameter, the host name can be abbreviated.

--
Example :
[user@localhost ~]\$ hrm --host=192.168.100.100 ...
--

1.5.10 port

=====

Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>

remote-port
Default : none
Range of Values : port number
=====

The service port number for the destination remote host is specified, which is applied to the path for the deletion target.

--
Example :
[user@localhost ~]\$ hrm --port=1874 ...
--

1.5.11 hcp-out

=====

Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>

output-path
Default : none
Range of Values : path string of file system
=====

The file to output the execution record of file deletion is set.

--
Example :
TARGET 127.0.0.1:11111:/home/user/Desktop/hcp_dst5
OK 0000 DE 00000001 ./
OK 0000 FR 00000002 ./file1.txt
OK 0000 DX 00000001 ./

Bytix Archaea tools Command Reference

EXIT 0 REASON 0000

--

FR (File Remove) means file deletion processing. DE (Directory Enter) means the confirmation proceeding whether it starts deleting directories which is done by setting the i option, DX (Directory eXit) means whose confirmation processing.

--

Example :

```
[user@localhost ~]$ hrm --hcp-out=- ...
```

--

1.6 hcp-ls

Usage: hcp-ls [OPTION]... [USER@]HOST[:PORT][:FILE] [:FILE]...

or: hcp-ls [OPTION]... --host=HOST [--port=PORT] [--user=USER] [FILE]...

The hcp-ls command gets the file list on the remote servers (server or hcpd server).

abbreviation	option	outline
q	query-cmdname	the flag to query command names
o	cmd-options	command option
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	the version is shown.
	config-test	display the loaded outcome of input parameters and configuration file
h	help	the display command line help
	user	User name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form

		HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investifation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	selcct identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatiblity for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.6.1 q, query-cmdname

```
=====
Supported OS : Linux / Windows / Mac
Format : -q | --query-cmdname
=====
```

Command names on the command list operated on servers are queried. Either of the following commands is shown.

- ls (Linux)
- dir (Windows)

--

Example :

```
[user@localhost ~]$ hcp-ls -q ...
```

--

1.6.2 o, cmd-options

```
=====
Supported OS : Linux / Windows / Mac
Format : -o <options> | --cmd-options=<options>
-----
options
Default : none
Range of Values : parameter option for the ls or dir command.
=====
```

The command options are set. When they include the blank or "-", it should be quote.

--

Example :

```
[user@localhost ~]$ hcp-ls -o "-al" ...
```

--

1.6.3 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hcp-ls command version is shown.

--

Example :

```
[user@localhost ~]$ hcp-ls -V
hcp-ls client (hcp-ls) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36
WS 4.2.0-2)
```

--

1.6.4 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```


Bytix Archaea tools Command Reference

Display the input parameters for the hcp-ls command and the configuration information.

```
--
Example :
[user@localhost ~]$ hcp-ls --config-test
...

-- [Targets] -----
---
-- [Command Options] -----
---
query-cmdname      : disable
cmd-options        : -
host               : -
port               : -
user               : -
password           : -
version            : disable
help               : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate    : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER          : user
LOGNAME       : user
HCP_PASSWORD  :
HCP_WS_PROXY  :
-----
---
```

Bytix Archaea tools Command Reference

Please type '--config-test --config-test ...' for more details.

--

3. h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The hcp-ls command help line is shown.

--

Example :

```
[user@localhost ~]$ hcp-ls -h
```

--

1.6.5 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
```

remote-host

Default : none

Range of Values : IP address or host name

=====

The destination remote host is specified, which is applied to the path for the listed target. With this parameter, the host name can be abbreviated.

--

Example :

```
[user@localhost ~]$ hcp-ls --host=192.168.100.100 ...
```

--

1.6.6 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
```

remote-port

Default : none

Range of Values : port number

=====

The service port number for the destination remote host is specified, which is applied to the path for the listed target.

Bytix Archaea tools Command Reference

```
--  
Example :  
[user@localhost ~]$ hcp-ls --port=1874 ...  
--
```

1.6.7 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to output the execution record of file list acquirement is set. The execution result of the list is always output as standard output.

```
--
Example :
FILE 127.0.0.1:11111:/home/user/Desktop/hcp_dst5
--
```

```
--
Example :
[user@localhost ~]$ hcp-ls --hcp-out=- ...
--
```

1.7 hmkdir

Usage: hmkdir [OPTION]... [USER@]HOST[:PORT]:DIRECTORY [:DIRECTORY]...
or: hmkdir [OPTION]... --host=HOST [--port=PORT] [--user=USER] DIRECTORY...

The hmkdir command creates directories on the remote servers (server or hcpd server).

abbreviation	option	outline
p	parents	parents directory create flag
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	show the version
	config-test	show the loaded results of the input parameters and configuration file.
h	help	show the command line help.

	user	user name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investigation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	select identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.7.1 p, parents

```
=====
SupportedOS : Linux / Windows
Format : -p | --parents
=====
```

If the parents directory is not found in the indicated path, the parent directory is also automatically created. Without this option, errors will happen when the parent directory does not exist.

--

Example :

```
[user@localhost ~]$ hmkdir -p ...
```

--

1.7.2 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

Show the hmkdir command version.

--

Example :

```
[user@localhost ~]$ hmkdir -V
hmkdir client (hmkdir) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36
WS 4.2.0-2)
```

--

1.7.3 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

Bytix Archaea tools Command Reference

Display the input parameters for the hmkdir command and the configuration information.

```
--
Example :
[user@localhost ~]$ hmkdir --config-test
...

-- [Targets] -----
---
-- [Command Options] -----
---
parents      : disable
host         : -
port         : -
user         : -
password     : -
version      : disable
help         : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate    : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER      : user
LOGNAME   : user
HCP_PASSWORD :
HCP_WS_PROXY :
-----
---
```

Bytix Archaea tools Command Reference

Please type '--config-test --config-test ...' for more details.

--

1.7.4 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

Show the hmdir command line help.

--

Example :

```
[user@localhost ~]$ hmdir -h
```

--

1.7.5 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The destination remote host is specified, which is applied to the path for the listed target. With this parameter, the host name can be abbreviated.

--

Example :

```
[user@localhost ~]$ hmdir --host=192.168.100.100
```

--

1.7.6 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
remote-port
Default : none
Range of Values : port number
=====
```

The destination remote port is specified, which is applied to the path for the listed target.

```
--
Example :
[user@localhost ~]$ hmkdir --port=1874
--
```

1.7.7 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to output the execution record of creating directories is set.

```
--
Example :
[user@localhost ~]$ hmkdir --hcp-out=- ...
DIR0 127.0.0.1:1874:/home/user/Desktop/hcp_mkdir14
DIR1 127.0.0.1:1874:/home/user/Desktop/hcp_mkdir15
OK 0000 DC 00000001 /home/user/Desktop/hcp_mkdir14
OK 0000 DC 00000002 /home/user/Desktop/hcp_mkdir15
EXIT 0 REASON 0000
[user@localhost ~]$
--
```

```
--
Example :
[user@localhost ~]$ hmkdir --hcp-out=- ...
--
```

1.8 hpwd

Usage: hpwd [OPTION]... [USER@]HOST[:PORT]

The hpwd command shows working directories on the remote server (server or hcpd server).

abbreviation	option	outline
L	logical	logical path
P	physical	physical path (symbolic link resolved)
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	show the version.

	config-test	show the loaded results of the input parameters and configuration file.
h	help	show the command line help.
	user	user name
	password	password
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	investigation	investigation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	select identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.8.1 L, logical

```
=====
Supported OS : Linux / Windows / Mac
Format : -L | --logical
=====
```

The logical path is returned.

```
--
Example :
[user@localhost ~]$ hpwd -L ...
--
```

1.8.2 P, physical

```
=====
Supported OS : Linux / Windows / Mac
Format : -P | --physical
=====
```

The physical path is returned. The symbolic links are resolved. When neither the logical option nor physical option is set, it is operated as if this option is specified.

```
--
Example :
[user@localhost ~]$ hpwd -P ...
--
```

1.8.3 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hpwd command version is shown.

```
--
Example :
```

```
[user@localhost ~]$ hpwd -V
hpwd client (hpwd) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS
4.2.0-2)
--
```

1.8.4 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

Output the input parameters for the hpwd command and the configuration information.

```
--
Example :
[user@localhost ~]$ hpwd --config-test
...

-- [Command Options] -----
---
logical      : disable
physical     : enable (implicit)
user         : -
password     : -
version      : disable
help         : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts  : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hpc/id_rsa ~/.hpc/id_ecdsa ~/.hpc/id_ed25519 ]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate    : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
```

Bytix Archaea tools Command Reference

```
---
USER          : user
LOGNAME       : user
HCP_PASSWORD  :
HCP_WS_PROXY  :
-----
---
```

Please type '--config-test --config-test ...' for more details.

--

1.8.5 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

Show the hpwd command line help.

--

Example :

```
[user@localhost ~]$ hpwd -h
```

--

1.9 hmv

```
Usage: hmv [OPTION]... [USER@]HOST[:PORT]:SOURCE :DEST
or: hmv [OPTION]... [USER@]HOST[:PORT]:SOURCE [:SOURCE]... :DIRECTORY
or: hmv [OPTION]... --host=HOST [--port=PORT] [--user=USER] SOURCE DEST
T
or: hmv [OPTION]... --host=HOST [--port=PORT] [--user=USER] SOURCE...
DIRECTORY
```

The hmv commands are used to transfer files or directories to and from the remote server or hcpd server.

abbreviation	option	outline
f	force	force overwriting in the destination
i	interactive	interactive overwriting in the destination
N	no-overwrite	prohibited overwriting in the destination
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	the version is shown.
	config-test	display the loaded outcome of input parameters and configuration file

Bytix Archaea tools Command Reference

h	help	the display command line help
	user	User name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investifation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	selcect identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatiblity for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.9.1 f, force

```
=====
Supported OS : Linux / Windows / Mac
Format : -f | --force
=====
```

When the same file or directory exists in the destination, it is overwritten.

```
--
Example :
[user@localhost ~]$ hmv -f ...
--
```

1.9.2 i, interactive

```
=====
Supported OS : Linux / Windows / Mac
Format : -i | --interactive
=====
```

When the same file or directory exists in the destination, a confirmation for overwriting it is taken place.

```
--
Example :
[user@localhost ~]$ hmv -i ...
--
```

1.9.3 N, no-overwrite

```
=====
Supported OS : Linux / Windows / Mac
Format : -N | --no-overwrite
=====
```

When the same file or directory exists in the destination, the process is skipped without overwriting.

Bytix Archaea tools Command Reference

--

Example :

```
[user@localhost ~]$ hmv -N ...
```

--

1.9.4 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hmv command version is shown.

--

Example :

```
[user@localhost ~]$ hmv -V
hmv client (hmv) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS 4.
2.0-2)
```

--

1.9.5 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

The available parameter for the hmv commands and the configuration information are output.

--

Example :

```
[user@localhost ~]$ hmv --config-test
...
```

```
-- [Sources] -----
---
-- [Destination] -----
---
-- [Command Options] -----
---
force           : disable
interactive     : disable
no-overwrite    : disable
host            : -
port            : -
user            : -
password        : -
```

Bytix Archaea tools Command Reference

```
version      : disable
help        : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519 ]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate     : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER      : user
LOGNAME   : user
HCP_PASSWORD :
HCP_WS_PROXY :
-----
---
```

Please type '--config-test --config-test ...' for more details.

--

1.9.6 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The hmv command help is shown.

--

Example :

```
[user@localhost ~]$ hmv -h
```

--

1.9.7 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The remote host in the destination is specified. It is used for the path to set the source and the destination. With this parameter, the hostname of this parameter can be abbreviated.

```
--
Example :
[user@localhost ~]$ hmv --host=192.168.100.100 ...
--
```

1.9.8 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
remote-port
Default : none
Range of Values : port number
=====
```

The service port number for the remote host of the destination is set. It is also used for the path to identify the source and destination.

```
--
Example :
[user@localhost ~]$ hmv --port=1874 ...
--
```

1.9.9 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to output the execution record of moving directories is set.

```
--
Example :
[user@localhost ~]$ hmv --hcp-out=- ...
SRC0 127.0.0.1:1874:/home/user/Desktop/hcp_hmv01.txt
SRC1 127.0.0.1:1874:/home/user/Desktop/hcp_hmv02.txt
DST 127.0.0.1:1874:/home/user/Desktop/hcp_hmv_dir
OK 0000 FM 00000001 /home/user/Desktop/hcp_hmv01.txt
OK 0000 FM 00000002 /home/user/Desktop/hcp_hmv02.txt
EXIT 0 REASON 0000
[user@localhost ~]$
--
```

```
--
Example :
[user@localhost ~]$ hmv --hcp-out=- ...
--
```

1.10 hln

```
Usage: hln [OPTION]... [USER@]HOST[:PORT]:TARGET :LINK_NAME
       or: hln [OPTION]... [USER@]HOST[:PORT]:TARGET [:TARGET]... :DIRECTORY
       or: hln [OPTION]... --host=HOST [--port=PORT] [--user=USER] TARGET LIN
K_NAME
       or: hln [OPTION]... --host=HOST [--port=PORT] [--user=USER] TARGET...
DIRECTORY
```

The hln commands creates links for the files and directories on the remote server and hcpd server. These commands are not supported on Windows OS.

abbreviation	option	outline
f	force	force overwriting in the destination
i	interactive	interactive overwriting in the destination
N	no-dereference	disable the dereference of the directory for the symbolic link
s	symbolic	create symboloc link
L	logical	use the target path as a logic name (symbolic link is resolved)
P	physical	use the target path as a logic name (symbolic link isn't resolved)
	symlink-target-expand-relative	expand the target's relative path to an absolute path
	symlink-target-accept-	accept the target expansion (when server is

	expand-relative	an older versin)
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	the version is shown.
	config-test	display the loaded outcome of input parameters and configuration file
h	help	the display command line help
	user	User name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investifation mode
	multi-run	multi-run mode

	no-agent	don't use agent
	ident-select	select identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatibility for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.10.1 f, force

```
=====
Supported OS : Linux / Windows / Mac
Format : -f | --force
=====
```

When the same link exists in the destination, it is supposed to be overwritten without confirmation.

```
--
Example :
[user@localhost ~]$ hln -f ...
--
```

1.10.2 i, interactive

```
=====
Supported OS : Linux / Windows / Mac
Format : -i | --interactive
=====
```

When the same link name exists in the destination, whether the link which has already existed in the destination is deleted is confirmed before overwriting.

```
--
Example :
[user@localhost ~]$ hln -i ...
--
```

1.10.3 N, no-dereference

```
=====
Supported OS : Linux / Windows / Mac
Format : -N | --no-dereference
=====
```

With this option, in the case that the path specified as the link is a symbolic link to a directory, this link is processed without dereferencing. On the other hand, when this option is not specified, the link is created with the target file name in the directory. This option changes this behavior.

```
--
Example :
[user@localhost ~]$ hln -N ...
--
```

1.10.4 s, symbolic

```
=====
Supported OS : Linux / Windows / Mac
Format : -s | --symbolic
=====
```

Symbolic link is created.

```
--
Example :
[user@localhost ~]$ hln -s ...
--
```

1.10.5 L, logical

```
=====
Supported OS : Linux / Windows / Mac
Format : -L | --logical
=====
```

In the case of the hard link, the path for the target is regarded as the logical name. When the path is a symbolic link, resolved path is used.

```
--
Example :
[user@localhost ~]$ hln -L ...
--
```

1.10.6 P, physical

```
=====
Supported OS : Linux / Windows / Mac
```

Format : -P | --physical

=====

In the case of the hard link, the path for the target is regarded as the physical name.
When the path is a symbolic link, it is proceeded without being resolved.

--

Example :

```
[user@localhost ~]$ hln -P ...
```

--

1.10.7 symlink-target-expand-relative

=====

Supported OS : Linux / Windows / Mac

Format: --symlink-target-expand-relative

=====

When the target is a relative path, this option tells the server to expand the relative path to an absolute path from a user working directory (home directory as usual) when creating a symbolic link.

--

Example :

```
[user@localhost ~]$ hln --symlink-target-expand-relative ...
```

--

1.10.8 symlink-target-accept-expand-relative

=====

Supported OS : Linux / Windows / Mac

Format : --symlink-target-accept-expand-relative

=====

When the target is a relative path, this option tells the hln command to accept that the server expands the relative path to an absolute path. This option will works when the server is an old one and it dose not support to create symbolic links with relative paths in targets.

The hln command will stop without running when the server is enough older not to support to do and neither this option nor —symlink-target-expand-relative are specified.

--

Example :

```
[user@localhost ~]$ hln --symlink-target-accept-expand-relative ...
```

--

1.10.9 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hln command version is shown.

```
--
Example :
[user@localhost ~]$ hln -V
hln client (hln) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36 WS 4.
2.0-2)
--
```

1.10.10 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

The parameters and the configuration information for the hln command are output.

```
--
Example :
[user@localhost ~]$ hln --config-test
...

-- [Targets] -----
---
-- [Link Name or Directory] -----
---
-- [Command Options] -----
---
force          : disable
interactive     : disable
no-dereference : disable
symbolic       : disable
logical        : disable
physical       : enable (implicit)
host           : -
port           : -
user           : -
password       : -
version        : disable
help           : disable
-- [Configuration Parameters] -----
```

```

---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication       : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts  : 3
CompressLevel            : -1
StrictHostKeyChecking    : ask
IdentityFile             : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519 ]
MaxReceiveRate           : 1000000000000
MaxSendRate              : 1000000000000
MaxConnectionReceiveRate : 1000000000000
MaxConnectionSendRate    : 1000000000000
TransportTimeout         : 180 sec
AcceptableCryptMethod    : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod   : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER      : user
LOGNAME   : user
HCP_PASSWORD :
HCP_WS_PROXY :
-----
---
```

Please type '--config-test --config-test ...' for more details.

--

1.10.11 h, help

```

=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The hln command help is shown.

--

Example :

```
[user@localhost ~]$ hln -h
```

--

1.10.12 host

```

=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
```



```
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The remote host in the destination is specified. It is used in the path specifies the link target, link name, or the directory. With this parameter, the host name for this path can be omitted.

```
--
Example :
[user@localhost ~]$ hln --host=192.168.100.100 ...
--
```

1.10.13 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
```

```
remote-port
Default : none
Range of Values : port number
=====
```

The service port number for the remote host in the destination is specified. It is used in the path specifies the link target, link name, or the directory.

```
--
Example :
[user@localhost ~]$ hln --port=1874 ...
--
```

1.10.14 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
```

```
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to output the execution record of creating links is set.

```
--
Example :
[user@localhost ~]$ hln --hcp-out=- ...
```

```
TARGET0 127.0.0.1:1874:/home/user/Desktop/hcp_hln01.txt
TARGET1 127.0.0.1:1874:/home/user/Desktop/hcp_hln02.txt
LINK_NAME/DIR 127.0.0.1:1874:/home/user/Desktop/hcp_hln_dir
OK 0000 FL 00000001 /home/user/Desktop/hcp_hln01.txt
OK 0000 FL 00000002 /home/user/Desktop/hcp_hln02.txt
EXIT 0 REASON 0000
[user@localhost ~]$
--
```

Example :

```
[user@localhost ~]$ hln --hcp-out=- ...
--
```

1.11 hchmod

```
Usage: hchmod [OPTION]... MODE[,MODE...] [USER@]HOST[:PORT]:FILE [:FILE
E]...
    or: hchmod [OPTION]... OCTAL-MODE [USER@]HOST[:PORT]:FILE [:FILE]...
    or: hchmod [OPTION]... --host=HOST [--port=PORT] [--user=USER] MODE[,M
ODE...] FILE...
    or: hchmod [OPTION]... --host=HOST [--port=PORT] [--user=USER] OCTAL-M
ODE FILE...
```

The hchmod command is a command to change permissions of files on the server. It is not supported on the Windows service.

abbreviation	option	outline
R	recursive	Change recursively
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	the version is shown.
	config-test	display the loaded outcome of input parameters and configuration file
h	help	the display command line help
	user	User name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-	show configuration option's names

	options	
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investifation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	selcct identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatiblty for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.11.1 R, recursive

```
=====
Supported OS : Linux / Windows / Mac
Format : -R | --recursive
=====
```

Changes permissions traversing directories recursively.

```
--
Example :
[user@localhost ~]$ hchmod -R ...
--
```

1.11.2 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hchmod command version is shown.

```
--
Example :
[user@localhost ~]$ hchmod -V
hchmod client (hchmod) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36
WS 4.2.0-2)
--
```

1.11.3 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

The parameters and the configuration information for the hchmod command are output.

```
--
Example :
[user@localhost ~]$ hchmod --config-test
...

-- [Targets] -----
---
-- [Command Options] -----
---
modes          : -
recursive      : disable
```

Bytix Archaea tools Command Reference

```
host          : -
port          : -
user          : -
password      : -
version       : disable
help          : disable
-- [Configuration Parameters] -----
---
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts  : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519 ]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate     : 100000000000
TransportTimeout          : 180 sec
AcceptableCryptMethod     : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod    : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER          : user
LOGNAME       : user
HCP_PASSWORD  :
HCP_WS_PROXY  :
-----
---
```

Please type '--config-test --config-test ...' for more details.

--

1.11.4 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The hchmod command help is shown.

--

Example :

```
[user@localhost ~]$ hchmod -h
--
```

1.11.5 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The remote host in the destination is specified. It is used in the path specifying the file. With this parameter, the host name for this path can be omitted.

```
--
Example :
[user@localhost ~]$ hchmod --remote-host=192.168.100.100 ...
--
```

1.11.6 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
remote-port
Default : none
Range of Values : port number
=====
```

The service port number for the remote host in the destination is specified. It is used in the path specifying the file.

```
--
Example :
[user@localhost ~]$ hchmod --remote-port=1874 ...
--
```

1.11.7 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
```

Range of Values : path string of file system

=====

The file to output the execution record of changing permissions is set.

--

Example :

```
[user@localhost ~]$ hchmod --hcp-out=- ...
HOST 127.0.0.1:1874
OK 0000 CA 00000001 hcp_dst/file1.txt
EXIT 0 REASON 0000
[user@localhost ~]$
```

--

--

Example :

```
[user@localhost ~]$ hchmod --hcp-out=- ...
```

--

1.12 hchown

Usage: hchown [OPTION]... OWNER[:[GROUP]] [USER@]HOST[:PORT]:FILE [:FILE]...

or: hchown [OPTION]... --host=HOST [--port=PORT] [--user=USER] OWNER[:[GROUP]] FILE...

The hchown command is a command to change owner or group of files on the server. It is not support on Windows service.

abbreviation	option	outline
d	no-dereference	disable the dereference of the directory for the symbolic link
R	recursive	changes recursively
s	follow-cmd-link-dir	follow symbolic links to directories on command line
S	follow-all	follow all symbolic links
D	no-follow	no follow symbolic links
	hpfp	HpFP protocol is used.
	wss	use the WebSocket protocol (SSL/TLS)
V	version	the version is shown.
	config-test	display the loaded outcome of input parameters and configuration file
h	help	the display command line help

	user	User name
	password	password
	host	remote host set
	port	remote port set
	config-file	configuration file
	config-option	make configuration from command line
	show-config-options	show configuration option's names
	hcp-diag	diagnostic log file
	stat-log-file	statistics log file
	udp	use the UDP (HpFP) protocol (bi-port form HpFP)
	ws	use the WebSocket protocol (plaintext communications)
	wss-no-check-certificate	SSL/TLS server certificate checking is disabled in WebSocket protocol
	ws-proxy-direct	not to use proxy servers
	ws-proxy	set the proxy server in the WebSocket protocol
	hpfp-cong	set the congestion control mode for the HpFP protocol
	hpfp-mss	set MSS for the HpFP protocol
	hpfp-sndbuf	set the sending buffer size for the HpFP protocol
	hpfp-rcvbuf	set the receiving buffer size for the HpFP protocol
	hcp-out	specify the file to output execution results
	investigation	investifation mode
	multi-run	multi-run mode
	no-agent	don't use agent
	ident-select	selcect identity
	include-conf-from-cwd	Include a path relative from cwd
	no-earlier-serv-compat	disable backward compatiblity for servers

Please refer to the hcpd command section on the following option.

--investigation

Please refer to the hcp command section on the following option.

--hpfp, --wss, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --stat-log-file, --udp, --ws, --wss-no-check-certificate, --ws-proxy-direct, --ws-proxy, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --multi-run, --no-agent, --ident-select, --include-conf-from-cwd, --no-earlier-serv-compat

1.12.1 d, no-dereference

```
=====
Supported OS : Linux / Windows / Mac
Format : -d | --no-dereference
=====
```

Change owner or group of files without resolving symbolic links. Changes will be applied to symbolic links.

```
--
Example :
[user@localhost ~]$ hchown -d ...
--
```

1.12.2 R, recursive

```
=====
Supported OS : Linux / Windows / Mac
Format : -R | --recursive
=====
```

Changes owner or group of files traversing directories recursively.

```
--
Example :
[user@localhost ~]$ hchown -R ...
--
```

1.12.3 s, follow-cmd-link-dir

```
=====
Supported OS : Linux / Windows / Mac
Format : -s | --follow-cmd-link-dir
=====
```

When symbolic links to directories are specified on the command line, change owner or group of files following the links.

Bytix Archaea tools Command Reference

--

Example :

```
[user@localhost ~]$ hchown -s ...
```

--

1.12.4 S, follow-all

```
=====
Supported OS : Linux / Windows / Mac
Format : -S | --follow-all
=====
```

Change owner or group of files following all symbolic links to directories.

--

Example :

```
[user@localhost ~]$ hchown -S ...
```

--

1.12.5 D, no-follow

```
=====
Supported OS : Linux / Windows / Mac
Format : -D | --no-follow
=====
```

Change owner or group of files without following symbolic links to directories.

--

Example :

```
[user@localhost ~]$ hchown -D ...
```

--

1.12.6 V, version

```
=====
Supported OS : Linux / Windows / Mac
Format : -V | --version
=====
```

The hchown command version is shown.

--

Example :

```
[user@localhost ~]$ hchown -V
hchown client (hchown) 1.5.13_2 / Linux (HpFP2 2.0.0.91_27 WSAPI 0.0.1.36
WS 4.2.0-2)
```

--

1.12.7 config-test

```
=====
Supported OS : Linux / Windows / Mac
Format : --config-test
=====
```

The parameters and the configuration information for the hchown command are output.

--

Example :

```
[user@localhost ~]$ hchown --config-test
```

...

```
-- [Targets] -----
```

```
-- [Command Options] -----
```

```
owner      : -
group      : -
no-dereference : disable
recursive  : disable
follow-cmd-link-dir : disable
follow-all : disable
no-follow   : enable
host        : -
port        : -
user        : -
password    : -
version     : disable
help        : disable
```

```
-- [Configuration Parameters] -----
```

```
PubkeyAuthentication      : yes
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [ ~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.s
sh/id_ed25519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519]
MaxReceiveRate            : 100000000000
MaxSendRate               : 100000000000
MaxConnectionReceiveRate  : 100000000000
MaxConnectionSendRate     : 100000000000
TransportTimeout          : 180 sec
```

Bytix Archaea tools Command Reference

```
AcceptableCryptMethod      : AES256/GCM AES256/CTR/VMAC AES256/CBC
AES128/CBC [Intel:AES-NI=yes]
AcceptableDigestMethod     : XXH3 SHA256 SHA160
-- [Environment Variables] -----
---
USER      : user
LOGNAME   : user
HCP_PASSWORD :
HCP_WS_PROXY :
-----
---

Please type '--config-test --config-test ...' for more details.
--
```

1.12.8 h, help

```
=====
Supported OS : Linux / Windows / Mac
Format : -h | --help
=====
```

The hchown command help is shown.

```
--
Example :
[user@localhost ~]$ hchown -h
--
```

1.12.9 host

```
=====
Supported OS : Linux / Windows / Mac
Format : --host=<remote-host>
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The remote host in the destination is specified. It is used in the path specifying the file. With this parameter, the host name for this path can be omitted.

```
--
Example :
[user@localhost ~]$ hchown --remote-host=192.168.100.100 ...
--
```

1.12.10 port

```
=====
Supported OS : Linux / Windows / Mac
Format : --port=<remote-port>
-----
remote-port
Default : none
Range of Values : port number
=====
```

The service port number for the remote host in the destination is specified. It is used in the path specifying the file.

```
--
Example :
[user@localhost ~]$ hchown --remote-port=1874 ...
--
```

1.12.11 hcp-out

```
=====
Supported OS : Linux / Windows / Mac
Format : --hcp-out=<output-path>
-----
output-path
Default : none
Range of Values : path string of file system
=====
```

The file to output the execution record of changing owner or group is set.

```
--
Example :
[user@localhost ~]$ hchown --hcp-out=- ...
HOST 127.0.0.1:1874
OK 0000 CA 00000001 hcp_dst/file1.txt
EXIT 0 REASON 0000
[user@localhost ~]$
--
```

```
--
Example :
[user@localhost ~]$ hchown --hcp-out=- ...
--
```

2 Configuration reference

2.1 hcpd.conf

hcpd daemon settings

setting item	explanation
ProtocolVersion	protocol version (fixed to 2)
TCPListenAddress	TCP service listen address setting
TCPServiceSocketSendBuffer	TCP sending buffer
HPFPListenAddress	HpFP service listen address
UDPListenAddress	HpFP service listen address (bi-port type)
UDPServiceExtensionBufferSize	HpFP service extension buffer size
WSSListenAddress	WebSocket(SSL/TLS) service listen address
WSSOptions	WSS options
WSSCipherSuites	WSS TLS 1.3 Cipher Suites
WSSCipherList	WSS TLS 1.2 or earlier Cipher Suites
WSListenAddress	WebSocket(no SSL/TLS) service listen address
ListenServiceBonding	listen service bonding
UseServerCertificateSecurity	enable server certificate security function
RequireServerCertificateSecurity	require server certificate security function
ServerKeyFile	server key file (If a “.pub” file exists, file transmissions are secured by both a private key and a public key.)
ServerCertificateFile	server certificate file
ServerCertificateChainFile	server certificate chain file
LocalPasswordAuthentication	local password authentication
PAMAuthentication	PAM authentication
PubkeyAuthentication	public key authentication
WinLogonUserAuthentication	Windows logon user authentication
MaxAuthTries	maximum number of authentication

	tries
PerformSystemAuthenticationRegardlessUsers	system authentication user setting
UserDirectoryFallbackAvailable	user directory fallback allowing
RejectOnUserHomeDirectoryNotFound	user home directory check
WinLogonUserNoRestrictedAccess	disable restricted access on Windows server
UsePrivilegeSeparation	privilege separation
PrivilegeSeparationMinimumUID	available minimum UID for privilege separation
PrivilegeSeparationMinimumGID	available minimum GID for privilege separation
PrivilegeSeparationUser	privilege separation default user
PrivilegeSeparationUmask	umask applied on privilege separation
PrivilegeSeparationUmaskAnonymous	umask applied on privilege separation (for anonymous)
ApplyUserPermission	apply the user permission
AllowUsers	POSIX users to accept
AllowGroups	POSIX groups to accept
DenyUsers	POSIX users to reject
DenyGroups	POSIX groups to reject
AuthorizedKeysSearchDir	authorized key search directory
AuthorizedKeysFile	authorized key file
AuthorizedKeysCommand	authorized key search command
AuthorizedKeysCommandUser	run user of the command
CACertificateFile	CA certificate file
CACertificatePath	CA certificate path (reserved)
CARevocationFile	CA CRL file
CARevocationPath	CA CRL searching directory (reserved)
OCSPRevocationEnabled	OCSP (Online Certificate Status Protocol)function
LocalUserFile	user configuration file
LocalPasswordFile	LPA authentication credentials file
AcceptableCryptMethod	acceptable crypt method

AcceptableDigestMethod	acceptable digest method
RequireDataIntegrityChecking	require data integrity checking
TransportCharEncoding	transport character encoding
HostEncoding	host character encoding
HeaderCompress	header compression (reserved)
ContentCompress	content compression (reserved)
MaxConcurrentThread	maximum current thread (Linux)
MaxTotalConnection	maximum total connection
MaxTcpConnection	maximum TCP connection
MaxUdpConnection	UDP (HpFP)connection limit
MaxWsConnection	WebSocket connection limit
MaxConnectionPerUser	maximum connection per user
MaxConnectionPerSec	maximum connection per second
MaxReceiveFileSize	maximum receiving file size
MaxSendFileSize	Maximum sending file size
MaxRequestFileEntryAtOnce	Max file entry request
MaxTotalBufferSize	Maximum buffer allocation size (entire system)
MaxBufferSizePerConnection	Maximum buffer allocation size (per connection)
MaxTotalReceiveRate	Maximum total receiving rate (entire system)
MaxTotalSendRate	Maximum total sending rate (entire system)
MaxReceiveRate	Maximum receiving rate (per session)
MaxSendRate	Maximum sending rate (per session)
MaxConnectionReceiveRate	Maximum receiving rate (per connection)
MaxConnectionSendRate	Maximum sending rate (per connection)
InitHeaderBlockSize	initial header block size
InitContentBlockSize	initial content block size
MaxHeaderBlockSize	maximum header block size
MaxContentBlockSize	mazimum content block size

FileLock	file lock
FileLockTrials	number of trials to lock files
FileLockTrialInterval	the trial interval (in seconds)
AtomicLikeSaving	atomically file saving
AtomicLikeSavingThreshold	threshold for atomically file saving
AtomicLikeSavingRejectOverwriteRequest	reject requests to overwriting temporary files which already exist when atomically file saving
TransportTimeout	transport timeout
IdleTimeout	idle timeout
DocPoint	document point (maximum file system access)
AccessList	access control list
SyslogOption	syslog option
SyslogFacility	syslog facility
SystemLog	log settings
SystemLogLevel	log level
ApplicationStatLog	application statistics
TransportStatLog	transport statistics
SystemStatLog	system statistics
FileOperationLog	file operation log
CallbackScript	call back script involved with applications
CallbackScriptHomeIsolation	call back script home isolation
CallbackScriptNoSymbolicLink	call back script ignores symbolic links
DisableMemoryManager	disable memory usage limitation for file payloads
DiskBenchmarkPreAllocation	how to make pre-allocation in disk benchmark
DiskBenchmarkPreAllocationSize	a unit size for the pre-allocation
DiskBenchmarkDirectAlignmentSize	Direct I/O benchmark, alignment size specification
DiskBenchmarkAsyncNoWait	Async I/O benchmark, NO_WAIT(reserved)

DiskBenchmarkAsyncMaxEvents	Async I/O benchmark, maximum number of I/O events at once
DiskBenchmarkAsyncMaxGetEvents	Async I/O benchmark, maximum number of taking event results at once
DiskBenchmarkAsyncRequestPoolSize	Async I/O benchmark, a size of pool holding request buffers
DeepDiskBenchmarkFileSize	file size on additional disk benchmarks
DeepDiskBenchmarkFreeSpaceRequired	required free space on the benchmarks
DeepDiskBenchmarkBlockSizes	a set of block sizes on the benchmarks
MemoryTransferConcurrency	concurrency memory copy configuration
MaxReadRate	Disk I/O reading rate per session
MaxWriteRate	Disk I/O writing rate per session
EnsureDestinationInFileTransfer	ensure to transfer files to the destination directory
StatLogPerUserInPrivilegeSeparation	statistics log output for privilege separation each user
NoSupplementalGroupInPrivilegeSeparation	disable supplemental groups on privilege separation
ApplicationStatLogSecurityEx	detailed security information output setting for application statistics logs
GetGrRMaxBufferSize	max buffer size for getgrxxx_r functions
GetPwRMaxBufferSize	max buffer size for getpwxxx_r functions

2.1.1 TCPListenAddress

```
=====
Supported OS : Linux.x86 / Windows
Format : TCPListenAddress <tcp_service_addr>[:<tcp_service_port>[:<mcd>]]
[ <acl_name>]
-----
tcp_service_addr
Default : none
Range of Values : IP address
```

```
-----
tcp_service_port
Format : <decimal_number>
Default : 874
Range of Values : decimal_number is 1-65535.
-----
```

```
mcd
Default : physical-CPU + 1, logical-CPU/2 + 1, 25 or 1
Range of Values : 1 - 65535
-----
```

```
acl_name
Default : none
Range of Values : name of access control list
=====
```

The available TCP services to allow to connect from client computers are defined.

tcp_service_addr is available IP address for TCP service.

tcp_service_port is available port for TCP service.

mcd is optional. This options specifies a number of connections provided for each client session on the service. When 1 is set, sessions will work with a single connection. When 2 or more are set, they will do with the number of connections. When you do not specify it, hcpd will determine a value from the number of physical cores, the number of logical cores and the license configuration.

- physical-CPU + 1 (physical-CPU < logical-CPU and physical-CPU > 1 under 25 maximum)

- logical-CPU/2 + 1 (physical-CPU = logical-CPU and logical-CPU/2 > 1 under 25 maximum)

- 1 (Otherwise. For example, the license dose not include this function or physical-CPU and logical-CPU do not meet the above conditions)

acl_name is a name of an access control list (see AccessList) that you would like to set to the TCP service. When this option is not set or the specified name is not found in access control lists, an unnamed access control list will be set to the TCP service.

```
--
Example :
TCPListenAddress 0.0.0.0:1874
--
```

2.1.2 TCPServiceSocketSendBuffer

```
=====
Supported OS : Linux.x86 / Windows
```

Format : TCPServiceSocketSendBuffer <snd-buf-size>

snd-buf-size

Format : <decimal_number>[[(T|G|M|K)]B]

Default : 0

Range of Values : unsigned double-length integer (byte)

=====

Specifies a TCP sending buffer size in bytes. 0 indicates no specification of this option.

You need this option to make a performance tuning of TCP on 100G environment. No need to use in ordinary cases.

--

Example :

TCPServiceSocketSendBuffer 128MB

--

2.1.3 HPFPListenAddress

=====

Supported OS : Linux.x86 / Windows

Format : HPFPListenAddress <hpfp_service_addr>[:<hpfp_service_port>[:<hpfp_sndbuf>[:<hpfp_rcvbuf>[:<hpfp_mss>[:<mcd>]]]]][<acl_name>]

hpfp_service_addr

Default : none

Range of Values : IP address

hpfp_service_port

Format : <decimal_number>

Default : 65520

Range of Values : decimal_number is 1-65535.

hpfp_sndbuf

Format : (DEFAULT | D | <decimal_number>[[(T|G|M|K)]B])

Default : 100MB

Range of Values : unsigned double-length integer (byte) D stands for DEFAULT.

hpfp_rcvbuf

Format : (DEFAULT | D | <decimal_number>[[(T|G|M|K)]B])

Default : 200MB

Range of Values : unsigned double-length integer (byte) D stands for DEFAULT.

hpfp_mss

Format : (DEFAULT | D | NONE | N | <decimal_number>[[(T|G|M|K)]B])

Bytix Archaea tools Command Reference

Default : NONE

Range of Values : unsigned integer (byte) D stands for DEFAULT. N stands for NONE.

mcd

Default : physical-CPU + 1, logical-CPU/2 + 1, 25 or 1

Range of Values : 1 - 65535

mcmp (Windows)

Default : no

Range of Values : yes, no

acl_name

Default : none

Range of Values : name of access control list
=====

The available HpFP services to allow to connect from client computers are defined.

hpfp_service_addr specifies the IP address for HpFP service.

hpfp_service_port is the port number of UDP transport for HpFP protocol in the optional setting.

hpfp_sndbuf is the transmission buffer size in the optional setting. "D" stands for default.

hpfp_rcvbuf is the buffer size for received data by HpFP protocol in the optional setting. "D" stands for default.

hpfp_mss is the MSS for HpFP protocol in the optional setting. "D" stands for default. In "N", the setting value is determined by the MTU searching using HpFP protocol.

mcd is optional. This option specifies a number of connections provided for each client session on the service. When 1 is set, sessions will work with a single connection. When 2 or more are set, they will do with the number of connections. When you do not specify it, hcpd will determine a value from the number of physical cores, the number of logical cores and the license configuration.

- physical-CPU + 1 (physical-CPU < logical-CPU and physical-CPU > 1 under 25 maximum)

- logical-CPU/2 + 1 (physical-CPU = logical-CPU and logical-CPU/2 > 1 under 25 maximum)

- 1 (Otherwise. For example, the license does not include this function or physical-CPU and logical-CPU do not meet the above conditions)

mcmp is optional. This option specifies whether Windows servers make the above session having multiple connections with multiple port numbers or not (single port). When you set this option to 'yes', the servers makes communication of HpFP protocol over other port numbers additional to the port number of it, e.g. a port range of 65520 - 65523 will be used when using the default port of 65520 and having 4 connections in the session. It is useful for cases where the session having multiple connections could not make an expected performance in throughput due to high CPU loads.

acl_name is an optional setting, as in TCP service.

```
--
Example :
HPFPListenAddress 0.0.0.0:10000
--
```

2.1.4 UDPListenAddress

```
=====
Supported OS : Linux.x86 / Windows
Format : UDPListenAddress <hpfp_service_addr>[:<hpfp_service_port>[:<hpfp_
udp_port>[:<hpfp_sndbuf>[:<hpfp_rcvbuf>[:<hpfp_mss>[:<mcd>]]]]]] [ <acl_n
ame>]
-----
hpfp_service_addr
Default : none
Range of Values : IP address
-----
hpfp_service_port
Format : <decimal_number>
Default : 884
Range of Values : decimal_number is 1-65535.
-----
hpfp_udp_port
Format : ( DEFAULT | D | <decimal_number> )
Default : 65520
Range of Values : decimal_number is 1-65535. D stands for DEFAULT.
-----
hpfp_sndbuf
Format : ( DEFAULT | D | <decimal_number>[[<(T|G|M|K)>]B] )
Default : 100MB
Range of Values : unsigned double-length integer (byte) D stands for DEFA
ULT.
-----
hpfp_rcvbuf
Format : ( DEFAULT | D | <decimal_number>[[<(T|G|M|K)>]B] )
Default : 200MB
Range of Values : unsigned double-length integer (byte) D stands for DEFA
ULT.
```

```
-----  
hfpf_mss  
Format : ( DEFAULT | D | NONE | N | <decimal_number>[[T|G|M|K]B] )  
Default : NONE  
Range of Values : unsigned integer (byte) D stands for DEFAULT. N stands  
for NONE.  
-----
```

```
mcd  
Default : physical-CPU + 1, logical-CPU/2 + 1, 25 or 1  
Range of Values : 1 - 65535  
-----
```

```
acl_name  
Default : none  
Range of Values : name of access control list  
=====
```

This option is deprecated.

The available HpFP (UDP) services to allow to connect from client computers are defined. This provides a manner of using HpFP services where a service's port number and a UDP transport's port number are defined respectively, but not a single UDP transport's number.

hfpf_service_addr specifies the IP address for HpFP service.

hfpf_service_port is a port number of the HpFP service in the optional setting.

hfpf_udp_port is the port number of UDP transport for HpFP protocol in the optional setting. "D" stands for default.

hfpf_sndbuf is the transmission buffer size in the optional setting. "D" stands for default.

hfpf_rcvbuf is the buffer size for received data by HpFP protocol in the optional setting. "D" stands for default.

hfpf_mss is the MSS for HpFP protocol in the optional setting. "D" stands for default. In "N", the setting value is determined by the MTU searching using HpFP protocol.

mcd is optional. This options specifies a number of connections provided for each client session on the service. When 1 is set, sessions will work with a single connection. When 2 or more are set, they will do with the number of connections. When you do not specify it, hcpd will determine a value from the number of physical cores, the number of logical cores and the license configuration.

- physical-CPU + 1 (physical-CPU < logical-CPU and physical-CPU > 1 under 25 maximum)

- $\text{logical-CPUs}/2 + 1$ (physical-CPUs = logical-CPUs and $\text{logical-CPUs}/2 > 1$ under 25 maximum)
- 1 (Otherwise. For example, the license dose not include this function or physical-CPUs and logical-CPUs do not meet the above conditions)

acl_name is an optional setting, as in TCP service.

--

Example :

```
UDPListenAddress 0.0.0.0:1884:10000
```

--

2.1.5 UDPServiceExtensionBufferSize

```
=====
Supported OS : Linux.x86 / Windows
Format : UDPServiceExtensionBufferSize <ext-buf-size>
-----
ext-buf-size
Default : 2GB
Range of Values : unsigned double-length integer (byte)
=====
```

The extension buffer size for HpFP (UDP) service is specified.

The size of the buffer for the traffic in the HpFP session is extended up to the specified size (hpfpsndbuf or hpfprcvbuf in UDPListenAddress) by adjusting to coincide with the increase of the latency, packet loss, and the volume of the traffic. The maximum total buffer size to extend is specified by this value.

When "0", this extension doesn't work.

The initial buffer size (the buffer size before extended) is 1MB.

--

Example :

```
UDPServiceExtensionBufferSize 4GB
```

--

2.1.6 WSSListenAddress

```
=====
Supported OS : Linux.x86 / Windows
Format : WSSListenAddress <wss_service_addr>[:<wss_service_port>[:<wss_op
t_name>[:<wss_cs_name>[:<wss_clist_name>[:<wss_privkey_name>[:<wss_cert_n
ame>[:<mcd>[:<use_hcpcm>]]]]]]]][:<acl_name>]
-----
wss_service_addr
Default : none
Range of Values : IP address
```

wss_service_port

Default : 443

Range of Values : port number

wss_opt_name

Format : (DEFAULT | D | <opt_name>)

Default : empty string

Range of Values : name of WSSOptions. D stands for DEFAULT.

wss_cs_name

Format : (DEFAULT | D | <cipher_suites_name>)

Default : empty string

Range of Values : name of WSSCipherSuites. D stands for DEFAULT.

wss_clist_name

Format : (DEFAULT | D | <cipher_list_name>)

Default : empty string

Range of Values : name of WSSCipherLlist. D stands for DEFAULT.

wss_privkey_name

Format : (DEFAULT | D | <server_key_file_name>)

Default : empty string

Range of Values : name of ServerKeyFile

wss_cert_name

Format : (DEFAULT | D | <server_cert_file_name>)

Default : empty string

Range of Values : name of ServerCertificateFile

mcd

Default : physical-CPU's + 1, logical-CPU's/2 + 1, 25 or 1

Range of Values : 1 - 65535

use_hcpcm

Default : no

Range of Values : yes, no

acl_name

Default : none

Range of Values : name of access control list
=====

The available WebSocket services (SSL/TLS) to allow to connect from client computers are defined.

wss_service_addr specifies the IP address for WebSocket service.

wss_service_port is available port for WebSocket service in the optional settings. A port number of 443 will be chosen when you omit this option.

wss_opt_name is optional. This option specifies a name of WSSOptions. D indicates the default value. When this is the empty string, the WSSOptions that dose not have any name will be chosen.

wss_cs_name is optional. This option specifies a name of WSSCipherSuites. D indicates the default value. When this is the empty string, the WSSCipherSuites that dose not have any name will be chosen.

wss_clist_name is optional. This option specifies a name of WSSCipherList. D indicates the default value. When this is the empty string, the WSSCipherList that dose not have any name will be chosen.

wss_privkey_name is optional. This option specifies a name of ServerKeyFile that includes a server key (a private key) for SSL/TLS communication. D indicates the default value. When this is the empty string, the ServerKeyFile that dose not have any names will be chosen.

wss_cert_name is optional. This option specifies a name of ServerCertificateFile that includes a server certificate for SSL/TLS communication. D indicates the default value. When this is the empty string, the ServerCertificateFile that dose not have any names will be chosen.

mcd is optional. This options specifies a number of connections provided for each client session on the service. When 1 is set, sessions will work with a single connection. When 2 or more are set, they will do with the number of connections. When you do not specify it, hcpd will determine a value from the number of physical cores, the number of logical cores and the license configuration.

- physical-CPUs + 1 (physical-CPUs < logical-CPUs and physical-CPUs > 1 under 25 maximum)

- logical-CPUs/2 + 1 (physical-CPUs = logical-CPUs and logical-CPUs/2 > 1 under 25 maximum)

- 1 (Otherwise. For example, the license dose not include this function or physical-CPUs and logical-CPUs do not meet the above conditions)

use_hcpcm is optional. This option enables encryption on application layer by AcceptableCryptMethod in addition to SSL/TLS communication. D indicates the default value.

acl_name is an optional setting, as in TCP service.

--

Example :

WSSListenAddress 0.0.0.0:8443

--

2.1.7 WSSOptions

Supported OS : Linux.x86 / Windows

Format : WSSOptions <opt_value>[<opt_name>]

opt_value

Format : (NONE | <openssl_opt_values>)

Default : NONE

Range of Values : list of SSL/TLS option names defined by OpenSSL

opt_name

Default : none

Range of Values : string

This option specified OpenSSL options that will be used on SSL/TLS communication.
Please use names described in the following URL.

https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_options.html
SSL_CTX_set_options

--

Example :

WSSOptions SSL_OP_NO_COMPRESSION:SSL_OP_NO_SSLv3

--

2.1.8 WSSCipherSuites

Supported OS : Linux.x86 / Windows

Format : WSSCipherSuites <cs_value>[<cs_name>]

cs_value

Format : (NONE | <openssl_cipher_suite_values>)

Default : NONE

Range of Values : list of Cipher Suites parameters defined by OpenSSL

cs_name

Default : none

Range of Values : string

This options specifie Cipher Suites parameters of OpenSSL that will be used on TLS
v1.3 communication. Please use names described in the following URL.

<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>
ciphers

Ciphte Suite names defined by "TLS v1.3 cipher suites"

--

Example :

WSSCipherSuites TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256

--

2.1.9 WSSCipherList

```
=====
Supported OS : Linux.x86 / Windows
Format : WSSCipherList <clist_value>[ <clist_name>]
-----
clist_value
Format : ( NONE | <openssl_cipher_list> )
Default : NONE
Range of Values : Cipher List parameters defined by OpenSSL
-----
clist_name
Default : none
Range of Values : string
=====
```

This option specifies Cipher List parameters of OpenSSL that will be used on SSL/TLS communication under TLS 1.2. Please use names described in the following URL.

<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>
ciphers

Cipher List in a format defined by "CIPHER LIST FORMAT2 and "CIPHER STRINGS".

--

Example :

WSSCipherList RC4-MD5:RC4-SHA:AES128-SHA:AES256-SHA:HIGH:!DSS:!aNULL

--

2.1.10 WSListenAddress

```
=====
Supported OS : Linux.x86 / Windows
Format : WSListenAddress <ws_service_addr>[:<ws_service_port>[:<mcd>]] [ <acl_name>]
-----
ws_service_addr
```

Default : none
Range of Values : IP address

ws_service_port
Default : 80
Range of Values : 1 - 65535

mcd
Default : physical-CPU + 1, logical-CPU/2 + 1, 25 or 1
Range of Values : 1 - 65535

acl_name
Default : none
Range of Values : name of access control list
=====

The available WebSocket services (no SSL/TLS) to allow to connect from client computers are defined.

ws_service_addr specifies an IP address for the WebSocket service.

ws_service_port specifies a port number of the WebSocket service.

mcd is optional. This options specifies a number of connections provided for each client session on the service. When 1 is set, sessions will work with a single connection. When 2 or more are set, they will do with the number of connections. When you do not specify it, hcpd will determine a value from the number of physical cores, the number of logical cores and the license configuration.

- physical-CPU + 1 (physical-CPU < logical-CPU and physical-CPU > 1 under 25 maximum)

- logical-CPU/2 + 1 (physical-CPU = logical-CPU and logical-CPU/2 > 1 under 25 maximum)

- 1 (Otherwise. For example, the license dose not include this function or physical-CPU and logical-CPU do not meet the above conditions)

acl_name is an optional setting, as in TCP service.

--
Example :
WSListenAddress 0.0.0.0:8080
--

2.1.11 ListenServiceBonding

=====

Supported OS : Linux / Windows
Format : ListenServiceBonding <service_name>[... <service_name>]

```
-----
service_name
Default : none
Range of Values : names of TCPListenAddress, HpFPListenAddress, etc.
=====
```

This specifies how hcpd makes bonding of services under multiple connection mode on sessions. Please specifies a name of service or names of services over which you want to make bonding of connections for sessions. You can see the names by -t option.

You can also use this option to make hybrid connections using TCP and HpFP for sessions.

Only one option can be described.

Clients connect to a server in ordinary way specifying the server host name and its port number of TCP or HpFP, etc. After the connection established, clients automatically make a number of new connections with the server up to the limit defined at services counting the first connection.

```
--
Example :
ListenServiceBonding tcp1 udp1
--
```

2.1.12 UseServerCertificateSecurity

```
=====
Supported OS : Linux.x86 / Windows
Format : UseServerCertificateSecurity <flag-available>
-----
```

```
flag-available
Default : yes
Range of Values : yes, no
=====
```

The server certificate security function is available. When “yes” is set, secured communications based on the PKI technology between clients are provided by the server certification specified in ServerCertificateFile or the public key resolved by the ServerKeyFile path.

```
--
Example :
UseServerCertificateSecurity no
--
```

2.1.13 RequireServerCertificateSecurity

```
=====
Supported OS : Linux.x86 / Windows
Format : RequireServerCertificateSecurity <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

Security communications for clients by server certification security function is available. When “yes” is set and the client requests the communication without this function (plain communication), the connection is denied.

```
--
Example :
RequireServerCertificateSecurity no
--
```

2.1.14 ServerKeyFile

```
=====
Supported OS : Linux.x86 / Windows
Format : ServerKeyFile <file-path>[ <serv-key-name>]
-----
file-path
Default :
    /etc/hcp/key/server.key (Linux.x86)
    C:/ProgramData/Clealink/HCP Tools/key/server.key (Windows)
Range of Values : path string of file system
-----
serv-key-name
Default : none
Range of Values : string
=====
```

The server private key path used in server certification security function is specified. When the public key exists in the private key path with the suffix “pub”, secured communications are provided by using this pair of keys, not by the setting of ServerCertificateFile.

server-key-name is optional. This option sets a name to the key. WSSListenAddress services use the name to refer to the key.

```
--
Example :
ServerKeyFile /etc/hcp/key/server.key
```

```
ServerKeyFile /etc/hcp/key/server.wss.key wss-key
--
```

When client users access the server for the first time, the following question is asked to make sure that the public key is registered as known_hosts.

```
A secure connection for host 127.0.0.1 can't be established.
RSA key fingerprint is SHA256: 0fzb9DY4qxXWPm/L/4cBKkk+FQ9577NIRYxRquZ6eW
A=.
Are you sure you want to continue connecting [yes/no] ?
```

By inputting “yes”, the key is supposed to be registered as a registered host in the path. In the case of the same public key of the same host, this procedure is skipped from next time.

```
<userhomedirectory>/etc/hcp/known_hosts (Linux)
<userhomedirectory>/_etc/hcp/known_hosts (Windows)
```

2.1.15 ServerCertificateFile

```
=====
Supported OS : Linux.x86 / Windows
Format : ServerCertificateFile <file-path>[ <serv-cert-name>]
-----
file-path
Default :
    /etc/hcp/cert/server.crt (Linux.x86)
    C:/ProgramData/Clealink/HCP Tools/cert/server.crt (Windows)
Range of Values : path string of file system
-----
serv-cert-name
Default : none
Range of Values : string
=====
```

the server certificate path is specified.

serv-cert-name is optional. This option sets a name to the certificate. WSSListenAddress use the name to refer to the certificate.

If you need intermediate certificates, please place certificates into the file in the order from the server certificate to the intermediate one.

```
--
Example :
ServerCertificateFile /etc/hcp/cert/server.crt
ServerCertificateFile /etc/hcp/cert/server.wss.crt wss-cert
--
```


2.1.16 ServerCertificateChainFile

```
=====
Supported OS : Linux.x86 / Windows
Format : ServerCertificateChainFile <file-path>
-----
file-path
Default :
    /etc/hcp/cert/server.crt (Linux.x86)
    C:/ProgramData/Clealink/HCP Tools/cert/chain.crt (Windows)
Range of Values : path string of file system
=====
```

Multiple intermediate certificates in the server certificate path are specified. Intermediate certificates are sent to clients in the order they are stored in the file after sending the server certificate.

```
--
Example :
ServerCertificateChainFile /etc/hcp/cert/chain.crt
--
```

2.1.17 LocalPasswordAuthentication

```
=====
Supported OS : Linux.x86 / Windows
Format : LocalPasswordAuthentication <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

LPA authentication is specified. LPA authentication is enabled by inputting "yes". If even one authentication is enabled including this authentication method of inputting "yes", the authentication is always required to access from clients. (Anonymous access prohibited)

```
--
Example :
LocalPasswordAuthentication yes
--
```

2.1.18 PAMAuthentication

```
=====
Supported OS : Linux
Format : PAMAuthentication <flag-available>
-----
flag-available
```

Default : yes
Range of Values : yes, no

=====

PAM authentication is specified. PAM authentication is enabled by inputting “yes”.

--
Example :
PAMAuthentication no
--

PAM authentication is valid for software distributed in RPM packages for Linux platforms.

PAM authentication depends on the system configuration. The PAM configuration files as below are appropriately configured according to the operating system environment where the service runs.

/etc/pam.d/hcpd

2.1.19 PubkeyAuthentication

=====

Supported OS : Linux.x86 / Windows
Format : PubkeyAuthentication <flag-available>

flag-available
Default : yes (Linux.x86), no (Windows)
Range of Values : yes, no

=====

Public key authentication is specified. It is enabled by inputting “yes”.

--
Example :
PubkeyAuthentication no
--

2.1.20 WinLogonUserAuthentication

=====

Supported OS : Windows
Format : WinLogonUserAuthentication <flag-available>

flag-available
Default : yes
Range of Values : yes, no

Windows authentication is specified. Windows authentication is enabled by inputting “yes”.

```
--  
Example :  
WinLogonUserAuthentication no  
--
```

Windows authentication is valid for software distributed in RPM packages for Windows platforms.

In the Windows authentication, the user ID and the password (including the domain name) will be just passed to the system standard API authentication function.

2.1.21 MaxAuthTries

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxAuthTries <max-tries>
-----
max-tries
Default : 6
Range of Values : signed integer
=====
```

This options specifies the number of authentication tries that the server accepts when users connect to it. It will respond a failure of authentication when all tries are not successful up to the number of tries.

If you specify 0 as this option, the server will respond the failure without any authentication tries. And it won't count tries when clients dose not send a request for authentication because of decryption failure of a private key or other reasons.

```
--  
Example :  
MaxAuthTries 3  
--
```

2.1.22 PerformSystemAuthenticationRegardlessUsers

```
=====
Supported OS : Linux.x86 / Windows
Format : PerformSystemAuthenticationRegardlessUsers <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

This option specifies wheter hcpd executes the system authentication (PAM or Windows Logon) regardless of the user definitions at /etc/hcp/users.

```
--  
Example :  
PerformSystemAuthenticationRegardlessUsers yes  
--
```

2.1.23 UserDirectoryFallbackAvailable

```
=====
Supported OS : Linux.x86 / Windows
Format : UserDirectoryFallbackAvailable <flag-available>
```

```
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

Whether to allow the fallbacks of the user home directory and the working directory is configured. When the home directory recognized as the registered authentication doesn't exist, whether to move backward to the directory described in the root document is specified. This option is invalid (no) in software version 1.1.0 and later on the client.

```
--
Example :
UserDirectoryFallbackAvailable yes
--
```

2.1.24 RejectOnUserHomeDirectoryNotFound

```
=====
Supported OS : Linux.x86 / Windows
Format : RejectOnUserHomeDirectoryNotFound <flag-available>
```

```
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

When the user home directory can't be found, whether to reject is set. This option is set to enable (yes) on the software before Ver.1.2.0.

```
--
Example :
RejectOnUserHomeDirectoryNotFound yes
--
```

2.1.25 WinLogonUserNoRestrictedAccess

```
=====
Supported OS : Windows
Format : WinLogonUserNoRestrictedAccess <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

This options switches how to make user's access on Windows servers with restricted access rights (without elevation of privilege) or not. When you set 'yes' on this option, the servers might apply elevated privileges to users belonging to the 'Administrators' group.

It is useful to avoid errors of accessing files or other resources due to access rights problem when users belonging to that group meet such errors. Please keep 'no' for this option normally.

```
--
Example :
WinLogonUserNoRestrictedAccess yes
--
```

2.1.26 UsePrivilegeSeparation

```
=====
Supported OS : Linux.x86 / Windows
Format : UsePrivilegeSeparation <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

The privilege separation for the client sessions is configured. In "yes", processing in the sessions is executed in a process different from the server standby process. In the divided processes, the user identification information (UID/GID and supplemental groups) based on the authentication result is set as user's access rights. If you want to change the specification of UID/GID from the default, please add an entry to /etc/hcp/users to overwrite it.

```
--
Example :
UsePrivilegeSeparation no
--
```

Supplemental groups can be applied up to 1000 groups. When they are over the number of groups, supplemental groups will be ignored (only UID and primary group GID applied). When the privilege separation is disabled, the processes on client sessions are operated following execution rights of each service.

On the Windows services, when authentication is performed by LPA or public key authentication rather than Windows logon authentication, client sessions works in the service's access rights (privilege separation will not applied to them).

2.1.27 PrivilegeSeparationMinimumUID

```
=====
Supported OS : Linux.x86
```

```
Format : PrivilegeSeparationMinimumUID <min-uid>
```

```
-----
min-uid
```

```
Default : 0
```

```
Range of Values : unsigned integer
=====
```

The minimum value of UID in which sessions can be executed in privilege separation enabled is configured, which is useful to control executions by users who has special rights.

This option will be disabled when the following options are configured.

- AllowUsers
- AllowGroups
- DenyUsers
- DenyGroups

```
--
```

```
Example :
```

```
PrivilegeSeparationMinimumUID 1000
```

```
--
```

2.1.28 PrivilegeSeparationMinimumGID

```
=====
Supported OS : Linux.x86
```

```
Format : PrivilegeSeparationMinimumGID <min-gid>
```

```
-----
min-gid
```

```
Default : 0
```

```
Range of Values : unsigned integer
=====
```

The minimum value of GID in which sessions can be executed in privilege separation enabled is configured, which is useful to control executions by users who has special rights.

This option will be disabled when the following options are configured.

- AllowUsers
- AllowGroups
- DenyUsers
- DenyGroups

--

Example :

PrivilegeSeparationMinimumGID 1000

--

2.1.29 PrivilegeSeparationUser

```
=====
Supported OS : Linux.x86 / Windows
Format : PrivilegeSeparationUser <username>
-----
username
Default : none
Range of Values : user names in the system
=====
```

In privilege separation working, the specified user's identification information will be applied when hcpd cannot determine any user's access rights to apply.

When user name isn't specified, a user name (nobody or everyone) depend on the platform is used.

--

Example :

PrivilegeSeparationUser nobody

--

2.1.30 PrivilegeSeparationUmask

```
=====
Supported OS : Linux.x86
Format : PrivilegeSeparationUmask <umask_val>[ <dir_umask_val>]
-----
umask_val
Default : 0022
Range of Values : from 0000 to 0777 in octal values
-----
dir_umask_val
```

Default : none
Range of Values : from 0000 to 0777 in octal values
- dir_umask_val is experimental.

=====

This option specifies a umask value applied to processes executing different from the server standby process on privilege separation.

umask_val specifies a umask value to apply. When dir_umask_val is not set, this value will be applied to both files and directories in the process.

dir_umask_val specifies a umask value to apply for directories. When this option is set, umask_val will be applied to files and dir_umask_val will be applied to directories. A common value of umask (umask_val & dir_umask_val) will be applied to the process and different from the common value will be applied respectively by HCP on creating files and directories. Please be careful of application of unexpected umask to files and directories which are not handled by HCP (so, this option is experimental).

If you want to set umask each user, please edit /etc/hcp/users.

--

Example :
PrivilegeSeparationUmask 0002

--

2.1.31 PrivilegeSeparationUmaskAnonymous

=====

Supported OS : Linux.x86
Format : PrivilegeSeparationUmaskAnonymous <umask_val>[<dir_umask_val>]

umask_val
Default : 0022
Range of Values : from 0000 to 0777 in octal values

dir_umask_val
Default : none
Range of Values : from 0000 to 0777 in octal values
- dir_umask_val is experimental.

=====

This option specifies a umask value applied to processes executing in anonymous different from the server standby process on privilege separation.

umask_val specifies a umask value to apply. When dir_umask_val is not set, this value will be applied to both files and directories in the process.

dir_umask_val specifies a umask value to apply for directories. When this option is set, umask_val will be applied to files and dir_umask_val will be applied to directories. A common value of umask (umask_val & dir_umask_val) will be applied to the process and different from the common value will be applied respectively by HCP on creating files and directories. Please be careful of application of unexpected umask to files and directories which are not handled by HCP (so, this option is experimental).

--

Example :

PrivilegeSeparationUmaskAnonymous 0022

--

2.1.32 ApplyUserPermission

```
=====
Supported OS : Linux.x86
Format : ApplyUserPermission <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When privilege separation isn't used, whether to use the authenticated user identification information (UID/GID) is applied for the file permission to the destination is configured.

--

Example :

ApplyUserPermission yes

--

2.1.33 AllowUsers

```
=====
Supported OS : Linux.x86
Format : AllowUsers [<username-pattern>...]
-----
username-pattern
Format : <name-pattern>[@<host-pattern>]
-----
name-pattern
Default : none
Range of Values : string including wildcards ('*' or '?')
-----
host-pattern
Default : none
Range of Values : CIDR form network address string
=====
```

This option specifies a name pattern of system users who are accepted to login (multiple specification is available).

username-pattern specifies a user name pattern and a CIDR form network address as option.

name-pattern specifies a pattern string representing user names. You can use a wildcard '*' representing any strings and another wildcard '?' representing any one character. When a user name input by a user matches with this pattern, hcpd accepts the login trial and performs authentication.

host-pattern specifies a CIDR form network address string. When the option is set, hcpd accepts the login trial if the name-pattern matches with the input user name and the network address includes the peer address of clients.

If hcpd confirms a pattern meets the above conditions, it terminates evaluation of patterns and accepts the login trial. When DenyUsers is also configured, the evaluation will be performed in the order from DenyUsers to AllowUsers. If no patterns meet the conditions when AllowUsers or AllowGroups are set, hcpd rejects the login trial.

The following configurations will be disabled when this option is set.

- PrivilegeSeparationMinimumUID
- PrivilegeSeparationMinimumGID

--

Example :

```
AllowUsers seg1-*@192.168.0.0/24
```

--

2.1.34 AllowGroups

```
=====
Supported OS : Linux.x86
Format : AllowGroups [<groupname-pattern>...]
-----
groupname-pattern
Default : none
Range of Values : string including wildcards ('*' or '?')
=====
```

This option specifies a name pattern of system groups who are accepted to login (multiple specification is available).

groupname-pattern specifies a pattern string representing group names. You can use a wildcard '*' representing any strings and another wildcard '?' representing any one character. When a primary group or supplemental groups the user belongs to matches with this pattern, hcpd accepts the login trial and performs authentication.

If hcpd confirms a pattern meets the above conditions, it terminates evaluation of patterns and accepts the login trial. When DenyGroups is also configured, the evaluation will be performed in the order from DenyGroups to AllowGroups. If no patterns meet the conditions when AllowUsers or AllowGroups are set, hcpd rejects the login trial.

The following configurations will be disabled when this option is set.

- PrivilegeSeparationMinimumUID
- PrivilegeSeparationMinimumGID

--

Example :

AllowGroups seg1-users

--

2.1.35 DenyUsers

Supported OS : Linux.x86

Format : DenyUsers [<username-pattern>...]

username-pattern

Format : <name-pattern>[@<host-pattern>]

name-pattern

Default : none

Range of Values : string including wildcards ('*' or '?')

host-pattern

Default : none

Range of Values : CIDR form network address string

=====

This option specifies a name pattern of system users who are rejected to login (multiple specification is available).

username-pattern specifies a user name pattern and a CIDR form network address as option.

name-pattern specifies a pattern string representing user names. You can use a wildcard '*' representing any strings and another wildcard '?' representing any one character. When a user name input by a user matches with this pattern, hcpd rejects the login trial and performs authentication.

host-pattern specifies a CIDR form network address string. When the option is set, hcpd rejects the login trial if the name-pattern matches with the input user name and the network address includes the peer address of clients.

When AllowUsers is also configured, the evaluation will be performed in the order from DenyUsers to AllowUsers. If a pattern meets the conditions, hcpd rejects the login trial without evaluating the remaining patterns.

The following configurations will be disabled when this option is set.

- PrivilegeSeparationMinimumUID
- PrivilegeSeparationMinimumGID

--

Example :

DenyUsers seg1-*@192.168.0.0/24

--

2.1.36 DenyGroups

```
=====
Supported OS : Linux.x86
Format : DenyGroups [<groupname-pattern>...]
-----
groupname-pattern
Default : none
Range of Values : string including wildcards ('*' or '?')
=====
```

This option specifies a name pattern of system groups who are rejected to login (multiple specification is available).

groupname-pattern specifies a pattern string representing group names. You can use a wildcard “*” representing any strings and another wildcard “?” representing any one character. When a primary group or supplemental groups the user belongs to matches with this pattern, hcpd rejects the login trial and performs authentication.

When AllowGroups is also configured, the evaluation will be performed in the order from DenyGroups to AllowGroups. If a pattern meets the conditions, hcpd rejects the login trial without evaluating the remaining patterns.

The following configurations will be disabled when this option is set.

- PrivilegeSeparationMinimumUID
- PrivilegeSeparationMinimumGID

--

Example :

DenyGroups guest-users

--

2.1.37 AuthorizedKeysSearchDir

```
=====
Supported OS : Linux.x86 / Windows
Format : AuthorizedKeysSearchDir <search-dir>
-----
search-dir
Default : NONE
Range of Values : path string of file system or NONE
=====
```

This option specifies a search directory to find out a user's public key for public key authentication. Please set NONE if you do not want to perform the search.

```
--
Example :
AuthorizedKeysSearchDir /etc/hcp/authkeys
--
```

The file name as below in the specified directory is searched as the file which the public key is stored in.

<user name>.pub

On the Linux platform, some files having writable permission on its Group and Other will be skipped with logging warnings.

The old name of 'AuthorizedKeySearchDir' is available.

2.1.38 AuthorizedKeysFile

```
=====
Supported OS : Linux.x86 / Windows
Format : AuthorizedKeysFile <file-path>
-----
file-path
Default :
(Linux.x86)
  ~/.ssh/authorized_keys
  ~/.hcp/authorized_keys
(Windows)
  ~/_hcp/authorized_keys
Range of Values : file path with a tilde which shows the user directory or NONE
=====
```

Specifies the key store file in the user home directory to find the user's public key for the public key authentication. Please set NONE if you do not want to perform the search.

On the Linux platform, some files having writable permission on its Group and Other will be skipped with logging warnings.

TOKENS of %2, %h, %U and %u is available defined under the following sshd_config.

https://man7.org/linux/man-pages/man5/sshd_config.5.html

TOKENS - AuthorizedKeysFile

Multiple entries are available separated with whitespaces or describing two or more configuration entries.

AuthorizedKeysFile ~/.ssh/my_authorized_keys2 ~/.hcp/my_authorized_keys2

AuthorizedKeysFile ~/.ssh/my_authorized_keys3

AuthorizedKeysFile ~/.hcp/my_authorized_keys3

The old name of 'AuthorizedKeyFile' is available.

2.1.39 AuthorizedKeysCommand

```
=====
Supported OS : Linux.x86
Format : AuthorizedKeysCommand <cmd-path>
-----
cmd-path
Default : none
Range of Values : command (or script) path to search for user's public keys
=====
```

Specifies the path of command (or script) to find the user's public key for the public key authentication. A username will be given to the command as the first argument. If you enable this configuration, hcpd requires AuthorizedKeysCommandUser.

--

Example :

AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys

--

TOKENS of %2, %h, %U and %u is available defined under the following sshd_config.

https://man7.org/linux/man-pages/man5/sshd_config.5.html

TOKENS - AuthorizedKeysCommand

2.1.40 AuthorizedKeysCommandUser

```
=====
Supported OS : Linux.x86
Format : AuthorizedKeysCommandUser <username>
-----
```

username

Default : none

Range of Values : user name that runs the command to search for user's public keys

=====

Specifies the user name that runs the command, specified by AuthorizedKeysCommand, to find the user's public key.

--

Example :

AuthorizedKeysCommandUser nobody

--

In general, it is recommended to use a user that works only for finding the public key and does not have any other role on the system.

https://man7.org/linux/man-pages/man5/sshd_config.5.html

AuthorizedKeysCommandUser

2.1.41 CACertificateFile

=====

Supported OS : Linux.x86 / Windows

Format : CACertificateFile <file-path>

file-path

Default :

/etc/hcp/cacert.pem (Linux.x86)

C:/ProgramData/Clealink/HCP Tools/cacert.pem (Windows)

Range of Values : path string of file system

=====

The file where CA certificate and intermediate certificate for client authentication are stored is configured.

--

Example :

CACertificateFile /etc/hcp/cacert.pem

--

The certificate in the PEM format is supported.

2.1.42 CACertificatePath (reserved)

=====

Supported OS : Linux.x86 / Windows

Format : CACertificatePath <dir-path>

dir-path

Default :

/etc/ssl (Linux.x86)

C:/ProgramData/Clealink/HCP Tools/ssl (Windows)

Range of Values : path string of file system

=====

The directory where CA certificate and intermediate certificate for client authentication are stored is configured.

--

Example :

CACertificatePath /etc/ssl

--

The certificate in the PEM format is supported.

2.1.43 CARevocationFile

=====

Supported OS : Linux.x86 / Windows

Format : CARevocationFile <file-path>

file-path

Default :

/etc/hcp/crl.pem (Linux.x86)

C:/ProgramData/Clealink/HCP Tools/crl.pem (Windows)

Range of Values : path string of file system

=====

The file where CRL for client authentication is stored is configured.

--

Example :

CARevocationFile /etc/hcp/crl.pem

--

The certification revocation list (CRL) in the PEM format is supported.

2.1.44 CARevocationPath (reserved)

=====

Supported OS : Linux.x86 / Windows

Format : CARevocationPath <dir-path>

dir-path

Default :

/etc/ssl (Linux.x86)

C:/ProgramData/Clealink/HCP Tools/ssl (Windows)

Range of Values : path string of file system

=====

the directory where CRL for client authentication is stored is configured.

```
--  
Example :  
CARevocationPath /etc/ssl  
--
```

The certification revocation list (CRL) in the PEM format is supported.

2.1.45 OCSPRevocationEnabled

```
=====
Supported OS : Linux.x86 / Windows
Format : OCSPRevocationEnabled <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

OCSP (Online Certificate Status Protocol) for client authentication is configured. It is enabled by inputting “yes”.

```
--  
Example :  
OCSPRevocationEnabled no  
--
```

2.1.46 LocalUserFile

```
=====
Supported OS : Linux.x86 / Windows
Format : LocalUserFile <file-path>[ <usage>]
-----
file-path
Default :
    /etc/hcp/users (Linux.x86)
    C:/ProgramData/Clealink/HCP Tools/users (Windows)
Range of Values : path string of file system
-----
usage
Default : overwrite
Range of Values : overwrite, define
=====
```

The file which defines the user information is configured.

file-path specifies a path of the file.

usage specifies how to use the file from the following options.

- overwrite
- define

When overwrite is set, the file will be used to overwrite how to authenticate users.

When define is set, hcpd recognizes users described in the file are available to login. So it rejects users who are not described in the file.

```
--  
Example :  
LocalUserFile /etc/hcp/users define  
--
```

2.1.47 LocalPasswordFile

```
=====
Supported OS : Linux.x86 / Windows
Format : LocalPasswordFile <file-path>
-----
file-path
Default :
    /etc/hcp/passwd (Linux.x86)
    C:/ProgramData/Clealink/HCP Tools/passwd (Windows)
Range of Values : path string of file system
=====
```

The file which defines the user credentials (password hash) used in LPA authentication is configured.

```
--
Example :
LocalPasswordFile /etc/hcp/passwd
--
```

2.1.48 AcceptableCryptMethod

```
=====
Supported OS : Linux.x86 / Windows
Format : AcceptableCryptMethod <method-names>
-----
method-names
Format : <method-name>[ ...]
Default : AES256/GCM AES256/CTR/VMAC AES256/CBC AES128/CBC
-----
method-name
Range of Values : PLAIN, AES128/CBC, AES192/CBC, AES256/CBC, AES128/CBC/H
MAC,
AES192/CBC/HMAC, AES256/CBC/HMAC, AES128/CBC/VMAC, AES192/CBC/VMAC,
AES256/CBC/VMAC, AES128/CBC/VMAC64, AES192/CBC/VMAC64, AES256/CBC/VMAC64,
```

AES128/CTR/HMAC, AES192/CTR/HMAC, AES256/CTR/HMAC, AES128/CTR/VMAC,
AES192/CTR/VMAC, AES256/CTR/VMAC, AES128/CTR/VMAC64, AES192/CTR/VMAC64,
AES256/CTR/VMAC64, AES128/GCM, AES192/GCM, AES256/GCM

=====

The cryptographic algorithm is configured.

When specified AES128/CBC, it is interpreted as AES128/CBC/HMAC.(They are the same algorithm. AES192/CBC and AES256/CBC are as well.)

When communicating with a host with versions that do not support the new algorithms, such as CTR/GCM mode and VMAC mode, these new algorithms that don't match the other host are ignored in the connection negotiation. However, still, the communications don't go to errors.

CTR/VMAC or GCM are recommended on network over 1Gbps, e.g. AES256/GCM, AES256/CTR/VMAC. Encrypted communication using CBC or HMAC, e.g. AES256/CTR/HMAC, AES256/CBC/HMAC, might make a bottle neck in performance on network over 1Gbps generally. VMAC64 checks data integrity with 64 bit, less than 128 bit in VMAC mode, which leads to better performance but less secured data integrity.

--

Example :

AcceptableCryptMethod AES256/CBC PLAIN

--

It is used to encrypt the messages communicated with a client. The algorithm is chosen to match the client configuration.

2.1.49 AcceptableDigestMethod

=====

Supported OS : Linux.x86 / Windows

Format : AcceptableDigestMethod <method-names>

method-names

Format : <method-name>[...]

Default : XXH3 SHA256 SHA160

method-name

Range of Values : NONE, SHA160, SHA224, SHA256, SHA384, SHA512, MD5, MM32, MM128,

XXH3, XXH128, XXH64, XXH32

=====

The digest algorithm is configured.

```
--  
Example :  
AcceptableDigestMethod SHA256 SHA160 NONE  
--
```

It is used to verify the messages, files, and data blocks communicated between clients. The algorithm which is consistent with the one in the client configuration is chosen.

In the case of encryption communications using HMAC like AES256/CBC/HMAC, the algorithms (MD5, MM32, MM128, XXH3, XXH128, XXH64, XXH32) other than the security digest algorithms are regarded as nothing configured.

MM32 and MM128 are discarded (, but its definition is kept for configuration compatibility). Please use XXH3 instead.

2.1.50 RequireDataIntegrityChecking

```
=====
Supported OS : Linux.x86 / Windows
Format : RequireDataIntegrityChecking <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When encrypted communication between server and clients, whether the server requests to check the integrity of communicating data (Data integrity test) by MAC (Message Authentication Code) is set.

When “no”, in the case that clients request not to check the data, accept the request and keep communicating.

When “yes”, reject the request.

“yes” (default) is recommended. This command is used to improve the performance in encrypted communication. Please be aware of the risk that the communicating data is not supposed to be checked when elected “no.”

```
--  
Example :  
RequireDataIntegrityChecking no  
--
```

2.1.51 TransportCharEncoding

```
=====
Supported OS : Linux.x86 / Windows
Format : TransportCharEncoding <encodings>
```

```
-----  
encodings  
Format : <encoding>[ ...]  
Default : UTF8  
-----
```

```
encoding  
Range of Values : US-ASCII, UTF8, UTF16, UTF32  
=====
```

The string encoding method used in the transport is configured.

```
--  
Example :  
TransportCharEncoding UTF8 UTF16 US-ASCII  
--
```

It is applied to strings, such as file paths exchanged between clients. The encoding which is consistent with the one in the client configuration is chosen.

2.1.52 HostEncoding

```
=====
```

```
Supported OS : Linux.x86 / Windows  
Format : HostEncoding <encoding>  
-----
```

```
encoding  
Default :  
  UTF-8 (Linux)  
  CP932 (Windows)  
Range of Values : encoding name supported by system and encoding conversion library (platform-dependent)  
=====
```

The string encoding method for the host computer is configured.

```
--  
Example :  
HostEncoding EUC-JP  
--
```

It is used to translate file paths into inner strings descriptions for the software.

2.1.53 HeaderCompress (reserved)

2.1.54 ContentCompress (reserved)

2.1.55 MaxConcurrentThread

```
=====
```

```
Supported OS : Linux.x86
```

Format : MaxConcurrentThread <max-threads>

max-threads

Default : 0

Range of Values : signed integer

=====

The maximum number of threads is configured.

2.1.56 MaxTotalConnection

=====

Supported OS : Linux.x86 / Windows

Format : MaxTotalConnection <max-total-con>

max-total-con

Default : 150

Range of Values : signed integer

=====

The maximum number of connections is configured.

--

Example :

MaxTotalConnection 5

--

2.1.57 MaxTcpConnection

=====

Supported OS : Linux.x86 / Windows

Format : MaxTcpConnection <max-tcp-con>

max-tcp-con

Default : 50

Range of Values : signed integer

=====

The maximum number of TCP connections is configured.

--

Example :

MaxTcpConnection 5

--

2.1.58 MaxUdpConnection

=====

Supported OS : Linux.x86 / Windows

Format : MaxUdpConnection <max-udp-con>

```
max-udp-con
Default : 50
Range of Values : signed integer
=====
```

The maximum number of HpFP (UDP) connections is configured.

```
--
Example :
MaxUdpConnection 5
--
```

2.1.59 MaxWsConnection

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxWsConnection <max-ws-con>
-----
```

```
max-ws-con
Default : 50
Range of Values : signed integer
=====
```

The maximum number of WebSocket connections is configured.

```
--
Example :
MaxWsConnection 5
--
```

2.1.60 MaxConnectionPerUser

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxConnectionPerUser <max-con-per-user>
-----
```

```
max-con-per-user
Default : 50
Range of Values : signed integer
=====
```

The maximum number of connections by each user is configured.

```
--
Example :
MaxConnectionPerUser 1
--
```

2.1.61 MaxConnectionPerSec

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxConnectionPerUser <max-con-per-user>
-----
max-con-per-user
Default : 50
Range of Values : signed integer
=====
```

The maximum number of connections per second is configured.

```
--
Example :
MaxConnectionPerSec 10
--
```

2.1.62 MaxReceiveFileSize

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxReceiveFileSize <file-size>
-----
file-size
Default : 8EB - 1B (Unlimited. The maximum value of signed double-length
integer)
Range of Values : signed double-length integer
=====
```

The maximum file size to allow to receive is configured.

```
--
Example :
MaxReceiveFileSize 1GB
--
```

2.1.63 MaxSendFileSize

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxSendFileSize <file-size>
-----
file-size
Default : 8EB - 1B (Unlimited. The maximum value of signed double-length
integer)
Range of Values : signed double-length integer
=====
```

The maximum file size to allow to send is configured.

--

Example :

MaxSendFileSize 1GB

--

2.1.64 MaxRequestFileEntryAtOnce

=====

Supported OS : Linux.x86 / Windows

Format : MaxRequestFileEntryAtOnce <max-file-req-at-once>

max-file-req-at-once

Default : 50

Range of Values : signed integer

=====

The maximum number of requested files to allow to send simultaneously is configured.

--

Example :

MaxRequestFileEntryAtOnce 1000

--

2.1.65 MaxTotalBufferSize

=====

Supported OS : Linux.x86 / Windows

Format : MaxTotalBufferSize <max-total-buf-size>

max-total-buf-size

Default : 4GB

Range of Values : signed double-length integer

=====

The maximum memory buffer size for file data processing on the hcpd daemon is configured.

--

Example :

MaxTotalBufferSize 8GB

--

2.1.66 MaxBufferSizePerConnection

=====

Supported OS : Linux.x86 / Windows

Format : MaxBufferSizePerConnection <max-buf-size-per-con>

max-buf-size-per-con

Default : 100MB

Range of Values : unsigned double-length integer

The maximum memory buffer size for file data processing by each client session is configured.

--

Example :

MaxBufferSizePerConnection 512MB

--

2.1.67 MaxTotalReceiveRate

Supported OS : Linux.x86 / Windows

Format : MaxTotalReceiveRate <bandwidth>

bandwidth

Default : 100Gbit

Range of Values : unsigned double-length integer

The traffic shaping control on the receiving bandwidth for the transport by the system (process) is configured.

--

Example :

MaxTotalReceiveRate 1Gbit

--

This function realizes the bandwidth control between the TCP/HpFP(UDP)/WebSocket layer and the application layer. When the value is over 10Gbps, it is processed as unlimited (without shaping). Other bandwidth shaping options are as well.

2.1.68 MaxTotalSendRate

Supported OS : Linux.x86 / Windows

Format : MaxTotalSendRate <bandwidth>

bandwidth

Default : 100Gbit

Range of Values : unsigned double-length integer

The traffic shaping control on the sending bandwidth for the transport by the system (process) is configured.

--

Example :

MaxTotalSendRate 1Gbit

--

2.1.69 MaxReceiveRate

=====

Supported OS : Linux.x86 / Windows

Format : MaxReceiveRate <bandwidth>

bandwidth

Default : 100Gbit

Range of Values : unsigned double-length integer

=====

The traffic shaping control on the receiving bandwidth for the transport by each client session is configured.

--

Example :

MaxReceiveRate 100Mbit

--

2.1.70 MaxSendRate

=====

Supported OS : Linux.x86 / Windows

Format : MaxSendRate <bandwidth>

bandwidth

Default : 100Gbit

Range of Values : unsigned double-length integer

=====

The traffic shaping control on the sending bandwidth for the transport by each client session is configured.

--

Example :

MaxSendRate 100Mbit

--

2.1.71 MaxConnectionReceiveRate

=====

Supported OS : Linux.x86 / Windows

Format : MaxConnectionReceiveRate <bandwidth>

bandwidth

Default : 100Gbit
Range of Values : unsigned double-length integer
=====

The traffic shaping control on the receiving bandwidth for the transport by each client connection is configured.

--
Example :
MaxConnectionReceiveRate 100Mbit
--

The old name of 'MaxReceiveRatePerConnection' is available.

2.1.72 MaxConnectionSendRate

=====

Supported OS : Linux.x86 / Windows
Format : MaxConnectionSendRate <bandwidth>

bandwidth
Default : 100Gbit
Range of Values : unsigned double-length integer
=====

The traffic shaping control on the sending bandwidth for the transport by each client connection is configured.

--
Example :
MaxConnectionSendRate 100Mbit
--

The old name of 'MaxSendRatePerConnection' is available.

2.1.73 InitHeaderBlockSize

=====

Supported OS : Linux.x86 / Windows
Format : InitHeaderBlockSize <block-size>

block-size
Default : 50KB
Range of Values : unsigned double-length integer
=====

The initial header block size is configured.

--
Example :

```
InitHeaderBlockSize 10KB
--
```

The maximum size of the header block including plural messages such as file request is given. This option is applied as soon as the transmission starts.

2.1.74 InitContentBlockSize

```
=====
Supported OS : Linux.x86 / Windows
Format : InitContentBlockSize <block-size>
-----
block-size
Default : 1MB
Range of Values : unsigned double-length integer
=====
```

The initial content block size is configured.

```
--
Example :
InitContentBlockSize 2MB
--
```

The maximum size of the header block including file data is given. This option is applied as soon as the transmission starts.

2.1.75 MaxHeaderBlockSize

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxHeaderBlockSize <block-size>
-----
block-size
Default : 50KB
Range of Values : unsigned double-length integer
=====
```

The maximum size of the header block to expand is configured.

```
--
Example :
MaxHeaderBlockSize 100KB
--
```

Once the transmission starts, the occupied bandwidth is measured and the header block size is changed into the available size.

2.1.76 MaxContentSize

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxContentSize <block-size>
-----
block-size
Default : 1MB
Range of Values : unsigned double-length integer
=====
```

The maximum size of the content block to expand is configured.

In environments over 10Gbps, when the communication performance hits a peak by making the most of it, changing MaxContentSize along with InitContentSize may reach an even better performance.

```
--
Example :
MaxContentSize 4MB
--
```

Once the transmission starts, the occupied bandwidth is measured and the content block size is changed into the available size.

2.1.77 FileLock

```
=====
Supported OS : Linux.x86 / Windows
Format : FileLock <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

In writing /reading files, whether to use the file lock is configured.

When yes is set, hcp acquires a file lock to write to files and read from them. On the Linux platform, this locking mechanism works well among softwares which use the same one since it is advisory lock.

When it is “no”, hcp dose not acuire the lock to do. This option is usable when some hang-ups occurs on network filesystems like NFS or some errors occurs on acquiring file locks. Please be careful of conflicts on destinations when multiple hcp commands run at one time.

When the lock request is processed properly and in waiting just to acquire the lock, the following log will be recorded (FileLockRetries is 0) or the processing will be stopped by detecting the maximum number of trials (FileLockRetries is more than 0).

```
2018/07/05 16:34:10 00007f638bd97740:INFO :Acquiring a lock to the file w
as rejected at the first trial.
```

```
2018/07/05 16:34:13 00007f638bd97740:INFO :Acquiring a lock to the file c
ontinues to be rejected about few seconds.
```

The operation is stopped by detecting the attempts have reached to the maximum number (FileLockRetries is over 0).

--

Example :

```
FileLock yes
```

--

2.1.78 FileLockTrials

```
=====
Supported OS : Linux.x86 / Windows
Format : FileLockTrials <num-trials>
-----
num-trials
Default : 0
Range of Values : unsigned integer
=====
```

The number of the maximum trials of acquiring the file lock is set. When 0, it is locked until the file lock acquired.

--

Example :

```
FileLockTrials 5
```

--

The old name of 'FileLockRetries' is available.

2.1.79 FileLockTrialInterval

```
=====
Supported OS : Linux.x86 / Windows
Format : FileLockTrialInterval <trial-interval>
-----
trial-interval
Default : 3
Range of Values : unsigned integer
=====
```

The interval time to request the file lock is set (sec).

```
--  
Example :  
FileLockTrialInterval 10  
--
```

The old name of 'FileLockRetryInterval' is available.

2.1.80 AtomicLikeSaving

```
=====
supported OS: Linux.x86 / Windows
Format : AtomicLikeSaving <flag-available> <temp-file-suffix>[ <temp-file
-prefix>]
-----
flag-available
Default : no
Range of Values : yes, no
-----
temp-file-suffix
Default : .tmp
Range of Values : up to 16 characters, NONE, RANDn
-----
temp-file-prefix
Default : NONE
Range of Values : up to 16 characters, NONE, RANDn
=====
```

It configures the settings for atomically file saving (two-step file saving by creating a temporary file) when transferring files.

flag-available specifies enabled/disabled for atomically file saving.

temp-file-suffix specifies the suffix of temporary files created when enabled. When "NONE", the suffix is not added.

temp-file-prefix specifies the prefix of temporary files created when enabled. When "NONE", the suffix is not added.

On the Linux versions, the write access right in the final destination is checked before creating temporary files.

With the resume function (-r option), files transferred part of the way are transferred from the beginning.

When RANDn is set, a file name which dose not conflict to existing files will be produced using a random string.

2.1.81 AtomicLikeSavingThreshold

```
=====
upported OS: Linux.x86 / Windows
Format : AtomicLikeSavingThreshold <threshold>
-----
threshold
Default : 100KB
Range of Values : signed double-length integer
=====
```

The file size threshold is set to enable file saving atomically.

This setting does not cover files under the threshold. “0 bytes” means all files are covered.

2.1.82 AtomicLikeSavingRejectOverwriteRequest

```
=====
upported OS: Linux.x86 / Windows
Format : AtomicLikeSavingRejectOverwriteRequest <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

It configures whether to reject a request (specified by client’s setting) to overwrite temporary files created in atomically saving.

It should be set to “no” to accept overwriting requests when there is no risk of collision of the temporary file name, by checking the application rules on file name, and the prefix/suffix string.

2.1.83 TransportTimeout

```
=====
Supported OS : Linux.x86 / Windows
Format : TransportTimeout <timeout>
-----
timeout
Default : 180
Range of Values : unsigned integer
=====
```

The timeout in seconds of the transport is set. When communication data including Keep-Alive data is unreached in the specified time on a session, it will end closing its connections as it is supposed to be unavailable to continue communication.

0 indicates disabling the timeout.

--

Example :

TransportTimeout 60

--

2.1.84 IdleTimeout

=====

Supported OS : Linux.x86 / Windows

Format : IdleTimeout <timeout>

timeout

Default : 0 (no timeout)

Range of Values : unsigned integer

=====

The timeout in seconds of the idle time for a session is set. When operations (command basis execution) in connection to the server is not taken place for the specified time, the connection from the server is closed. It is applied when users operate simultaneously from remote by the terminal function (provided by API library), where user can input plural commands.

0 indicates disabling the timeout.

--

Example :

IdleTimeout 180

--

2.1.85 DocPoint

=====

Supported OS : Linux.x86 / Windows

Format : DocPoint <doc_point_name>

doc_point_name

Default : none

Range of Values : characters

=====

The document point is defined. doc_point_name shows the name of this document point.

When the user home directory can't be found, this document point is used as the home directory.

--

Example :

DocPoint /home

--

2.1.86 DocPath

```
=====
Supported OS : Linux.x86 / Windows
Format : DocPath <doc_path>
-----
doc_path
Default : none
Range of Values : path string of file system
=====
```

The directory path for the document point is specified.

--

Example :

DocPath /home

--

The access to the files and directories is permitted by this directory path.

2.1.87 HomeIsolation

```
=====
Supported OS : Linux.x86 / Windows
Format : HomeIsolation <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

User's home isolation is set on a document point.

--

Example :

HomeIsolation yes

--

When you specify this option to 'yes' and the path of this document point includes a path of the user home directory, access validation will be performed to the path of user home (home isolation), but not the path of this document point.

2.1.88 PermitAccessRead

```
=====
Supported OS : Linux.x86 / Windows
Format : PermitAccessRead <flag-available>
-----
```

flag-available

Default : no

Range of Values : yes, no

=====

The permission to read the files in the document point is set.

--

Example :

 PermitAccessRead yes

--

When “no” is set, the files in the document point are prohibited to read. For example, it makes reading errors of files on file transfer.

2.1.89 PermitAccessWrite

=====

Supported OS : Linux.x86 / Windows

Format : PermitAccessWrite <flag-available>

flag-available

Default : no

Range of Values : yes, no

=====

The permission to write the files in the document point is set.

--

Example :

 PermitAccessWrite yes

--

When “no” is set, the files in the document point are prohibited to write. For example, it makes writing errors of files on file transfer.

2.1.90 PermitAccessOverwrite

=====

Supported OS : Linux.x86 / Windows

Format : PermitAccessOverwrite <flag-available>

flag-available

Default : no

Range of Values : yes, no

=====

The permission to overwrite the files in the document point is set.

```
--
Example :
    PermitAccessOverwrite yes
--
```

When “no” is set, the files in the document point are prohibited to overwrite. For example, it makes errors on overwriting to files which already exist.

2.1.91 PermitAccessDelete

```
=====
Supported OS : Linux.x86 / Windows
Format : PermitAccessDelete <flag-available>
-----
```

```
flag-available
Default : no
Range of Values : yes, no
=====
```

The permission to delete the files in the document point is set.

```
--
Example :
    PermitAccessDelete yes
--
```

When “no” is set, the files in the document point are prohibited to delete.

2.1.92 PermitAccessRandomRead (reserved)

```
=====
Supported OS : Linux.x86 / Windows
Format : PermitAccessRandomRead <flag-available>
-----
```

```
flag-available
Default : no
Range of Values : yes, no
=====
```

The permission for the random read access in the document point is set.

```
--
Example :
    PermitAccessRandomRead yes
--
```

2.1.93 PermitAccessRandomWrite (reserved)

```
=====
Supported OS : Linux.x86 / Windows
Format : PermitAccessRandomWrite <flag-available>
```

```
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

The permission for the random write access in the document point is set.

```
--
Example :
    PermitAccessRandomRead yes
--
```

2.1.94 AccessList

```
=====
Supported OS : Linux.x86 / Windows
Format : AccessList <acl_name>
-----
```

```
acl_name
Default : none
Range of Values : characters
=====
```

The access control list is defined. acl_name is an optional setting. The access control list is specified.

```
--
Example :
AccessList acl1
--
```

When acl_name is not used, it is treated as the unnamed access control list. Only one unnamed access control list can be defined.

2.1.95 Allow

```
=====
Supported OS : Linux.x86 / Windows
Format : Allow (<ip_addr> <net_mask>|any)[ <hpf Cong_mode_modifier>]
-----
```

```
ip_addr
Default : none
Range of Values : IP address
-----
```

```
net_mask
Default : none
Range of Values : subnet mask
-----
```

```
hpfp_cong_mode_modifier
Format : <modifier>[...]
modifier := (+|-)(M|S|A|T)[...]
Default : none
=====
```

The access permission on the access control list is defined.

ip_addr is IP address.

net_mask is net mask.

“any” means all network.

hpfp_cong_mode_modifier specifies the overwriting of the HpFP congestion control mode.

In the HpFP congestion control mode, M, S, and A stands for MODEST, FAIR_FAST_START, and AGGRESSIVE respectively.

“+” means enabling the HpFP congestion control mode which is described after “+”, when the connection which matches with one of this allowed access list is received.

“-” means canceling the HpFP congestion control mode which is described after “-”.

```
--
Example :
    Allow 192.168.1.0 255.255.255.0 -A+M
--
```

When the input network includes the client IP address, it is allowed to be accessed.

2.1.96 Deny

```
=====
Supported OS : Linux.x86 / Windows
Format : Deny (<ip_addr> <net_mask>|any)
-----
```

```
ip_addr
Default : none
Range of Values : IP address
-----
```

```
net_mask
Default : none
Range of Values : subnet mask
=====
```

Denying to access is defined in the access control list.

```
--
Example :
    Deny 192.168.1.0 255.255.255.0
--
```

When the input network includes the client IP address, it is denied to be accessed.

2.1.97 SyslogOption

```
=====
Supported OS : Linux.x86 / Windows
Format : SyslogOption <syslog-options>
-----
syslog-options
Format : syslog-option[ ...]
Default : CONS PID
-----
syslog-option
Range of Values : CONS, NDELAY, NOWAIT, ODELAY, PERROR, PID
=====
```

Syslog option (or options) are configured.

Each option is available for syslog option with prefix "LOG_".

```
--
Example :
SyslogOption PID
--
```

2.1.98 SyslogFacility

```
=====
Supported OS : Linux.x86 / Windows
Format : SyslogFacility <syslog-facility>
-----
syslog-facility
Default : DAEMON
Range of Values : AUTH, CRON, DAEMON, FTP, LOCAL0 - LOCAL7, LPR, MAIL, NEWS, USER, UUCP
=====
```

Syslog facility is set.

Each facility is available for syslog facility with prefix "LOG_".

```
--
Example :
SyslogFacility FTP
--
```


2.1.99 SystemLog

```
=====
Supported OS : Linux.x86 / Windows
Format : SystemLog <log-level>[ <flag-available>][ <log-rotation-conf>][
<log-path>]
-----
log-level
Default : INFO
Range of Values : EMERG, ALERT, CRIT, ERR, WARNING, INFO, DEBUG
-----
flag-available
Default : yes
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
-----
log-path
Default : /var/log/hcpd.log
Range of Values : path string of file system
=====
```

System log settings

log-level is set.

When “yes” in flag-available, logs are output.

log-rotation-conf specifies on log rotation. When this option is not specified, log rotations don’t take place. When FileSize is set, log rotations take place setting the file-size to the threshold. When DatePattern is set, log rotations take place based on the date.

file-size specifies the threshold of the file size in bytes.

backups specifies the maximum number of generations for log rotation to store when FileSize is set.

date-pattern specifies the pattern of the log rotation based on the date.

When FileSize is set, the number of the generations is supposed to be added as the suffix to the pathname of the log files as follows during log rotation.

```
<specified path> // the path of the log currently being written
<specified path>.1
<specified path>.2
...
<specified path>.n // "n" is the number set in backups
```

When the number of the log rotations exceeds the number specified in “backups”, the exceeded generation’s files are deleted.

When DatePattern is specified, the time and date are supposed to be added as the suffix to the pathname of the log files, following the specified pattern during log rotation.

```
// in the case of yyyy-MM-dd
<specified path> // the path of the log currently being written
<specified path>.2019-12-10 // the log for 2019/12/10
<specified path>.2019-12-09
...
<<specified path>.2019-11-30
...
```

Log rotation takes place based on the unit of the specified pattern. In the month unit case, a log file records throughout that month, starting at 0:00 on the first day of that month and ending at right before 0:00 on the first day of the following month.

Example :

```
from 2019/11/01 00:00:00 to 2019/12/01 00:00:00
(It doesn't include 2019/12/01 00:00:00)
```

In the minute unit, a log file records throughout the minute, from 0 seconds in that minute to right before 0 seconds in the following minute.

Example :

```
from 2019/11/01 10:30:00 to 2019/11/01 10:31:00
(It doesn't include 2019/11/01 10:31:00)
```

After the specified duration, the log writing request triggers the log to rotate before the log writing. The log file is renamed by adding a suffix of that duration.

```
// yyyy-MM-dd-HH-mm rotation case
2019/12/10 00:00 the server starts
2019/12/10 00:05 the server stops
2019/12/10 00:07 the server restarts
...
--
<specified path>
<specified path>.2019-12-10-00-11
<specified path>.2019-12-10-00-10 // No record from 00:09 to 00:10
<specified path>.2019-12-10-00-08
<specified path>.2019-12-10-00-07 // recorded from the server-restart
<specified path>.2019-12-10-00-05 // recorded until the server-stop in 0
0:05 (In restarting, the log rotation is judged based on the update time
of the log file.)
...
<specified path>.2019-12-10-00-00
```

The server using the privilege separation rotates logs periodically (about each 128 ms). Therefore the log content which should be in the following file may be output in the current file, because rotations may be delayed due to this 128 ms delay.

log-path specifies the log path. When specified together with the command parameter “-l”, the command parameter is effective.

```
--
Example1 :
SystemLog WARNING FileSize 10MB 10
Example2 :
SystemLog WARNING DatePattern yyyy-MM-dd
Example3 :
SystemLog WARNING // the same as SystemLogLevel
--
```

2.1.100 SystemLogLevel

```
=====
Supported OS : Linux.x86 / Windows
Format : SystemLogLevel <log-level>
-----
log-level
Default : INFO
Range of Values : EMERG, ALERT, CRIT, ERR, WARNING, INFO, DEBUG
=====
```

The system log level is set, which does not affect any syslog functions.

When you describe SystemLog, this option override the log level.

```
--
Example :
SystemLogLevel WARNING
--
```

2.1.101 ApplicationStatLog

```
=====
Supported OS : Linux.x86 / Windows
Format : ApplicationStatLog <flag-available>[ <log-rotation-conf>]
-----
flag-available
Default : yes
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
=====
```

The configuration on the application statistics is set.

When “yes” in “flag-available”, the application statistics information is output.

log-rotation-conf specifies the rotation rule. It works in the same way as the rotation behavior set in “SystemLog”. However, unlike the “SystemLog” logs don’t rotate periodically when using the privilege separation.

Based on the paths specified in “FileSize” and “DatePatternas” as each criterion, the rotations are carried out as below.

```
// FileSize cases
<specified path>.application
<specified path>.application.1
<specified path>.application.2
...
<specified path>.application.n
```

```
// DatePattern cases
<specified path>.application
<specified path>.application.2019-12-10
<specified path>.application.2019-12-09
...
```

The header of the statistics information is not included in rotated files.

```
--
Example1 :
ApplicationStatLog no
Example2 :
ApplicationStatLog yes FileSize 10MB 10
Example3 :
ApplicationStatLog yes DatePattern yyyy-MM-dd
--
```

2.1.102 TransportStatLog

```
=====
Supported OS : Linux.x86 / Windows
Format : TransportStatLog <flag-available>[ <log-rotation-conf>]
-----
flag-available
Default : no
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
=====
```

The configuration on the transport statistics is set.

When “yes” in flag-available, the transport statistics data is output.

log-rotation-conf specifies the rotation rule. It works in the same way as the rotation behavior set in "SystemLog". When using the privilege separation, logs rotate periodically.

Based on the paths specified in "FileSize" and "DatePatternas" as each criterion, the rotations are carried out as below.

```
// FileSize cases
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>.1
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>.2
...
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>.n
// DatePattern cases
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>.2019-12-10
<specified path>.transport.tcp.service_<service number>.<service port number>.thread_<thread number>.2019-12-09
...
```

The header of the statistics information is not included in rotated files.

```
--
Example1 :
TransportStatLog yes
Example2 :
TransportStatLog yes FileSize 10MB 10
Example3 :
TransportStatLog yes DatePattern yyyy-MM-dd
--
```

2.1.103 SystemStatLog

```
=====
Supported OS : Linux.x86 / Windows
Format : SystemStatLog <flag-available>[ <log-rotation-conf>]
-----
flag-available
Default : yes
Range of Values : yes, no
-----
log-rotation-conf
```

```
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
=====
```

The configuration on the system statistics is set.

When “yes” in flag-available, the system statistics data is output.

log-rotation-conf specifies the rotation rule. It works in the same way as the rotation behavior set in “SystemLog”. However, unlike the “SystemLog” logs don’t rotate periodically when using the privilege separation.

Based on the paths specified in “FileSize” and “DatePatternas” as each criterion, the rotations are carried out as below.

```
// FileSize cases
<specified path>.system
<specified path>.system.1
<specified path>.system.2
...
<specified path>.system.n
// DatePattern cases
<specified path>.system
<specified path>.system.2019-12-10
<specified path>.system.2019-12-09
...
```

The header of the statistics information is not included in rotated files.

```
--
Example1 :
SystemStatLog yes
Example2 :
SystemStatLog yes FileSize 10MB 10
Example3 :
SystemStatLog yes DatePattern yyyy-MM-dd
--
```

2.1.104 FileOperationLog

```
=====
Supported OS : Linux.x86 / Windows
Format : FileOperationLog <flag-available>[ <log-rotation-conf>][ <log-path>]
-----
flag-available
Default : no
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
-----
log-path
Default : none
Range of Values : path string of file system
=====
```

The configuration on the file operation logging is set.

When “yes” in flag-available, the file operation logs are output.

log-rotation-conf specifies the rotation rule. It works in the same way as the rotation behavior set in “SystemLog”. When using the privilege separation, logs rotate periodically.

Based on the paths specified in “FileSize” and “DatePatternas” as each criterion, the rotations are carried out as below.

```
// FileSize cases
<log path>
<log path>.1
<log path>.2
...
<log path>.n
```



```
// DatePattern cases
<log path>
<log path>.2019-12-10
<log path>.2019-12-09
...
```

The header of the statistics information is not included in rotated files.

log-path specifies a path of a file to which you want to output file operation logs. When it is not set, the following value will be used.

```
/var/log/hcpd.file.operation.log (Linux.x86)
C:/ProgramData/Clealink/HCP Tools/hcpd.file.operation.log (Windows)
```

The file operation logs include the following I/O processing records.

- Finish of reading a file
- Finish of writing a file
- Remove a file (including removing by synchronization)
- Creation of a directory
- Rename a file
- Creation of a hard link
- Creation of a symbolic link
- List files

And the following records will be produced as records including acknowledgements by the application (HCP).

- Completion of a file upload
- Completion of a file download
- Completion of synchronization of files
- Completion of removing a file
- Completion of creating a directory
- Completion of renaming a file
- Completion of creating a hard link
- Completion of creating a symbolic link

The records include the following fields in common.

- Date and time
- Peer IP address and port number
- User name

Paths of files are recorded in the specification of each operation.

The format of the logs is in the following specification.

```
=====
Format:
yyyy/mm/dd HH:MM:SS.<usec> <remote-ip> <username> <hcp-operation-name>[ <
sub-operation-label>] <path>...
yyyy/mm/dd HH:MM:SS.<usec> <remote-ip> <username> <file-io-operation-name
>\[<hcp-operation-name>\] <path>...
-----
usec
Range of Values : micro seconds (000000 - 999999)
-----
remote-ip
Range of Values : peer IP address and port number
-----
username
Range of Values : User name and authentication method
-----
hcp-operation-name
Range of Values : FT, FS, FR, LR, DC, FM, FL
-----
sub-operation-label
Range of Values : U, D, H, S
-----
file-io-operation-name
Range of Values : FileRead, FileWritten, FileDeleted, DirectoryCreated,
FileRenamed, LinkCreated, SymbolicLinkCreated, ListFilesRawFormat
=====
```

hcp-operation-name indicates a type of the following applications.

- FT (File transfer)
- FS (Delete file on file synchronization)
- FR (File remove)
- LR (List files. Output of ls or dir)
- DC (Directory creation)
- FM (File move)
- FL (Link creation)

sub-operation-label indicates a sub type of some applications.

- U (Upload. Used in FT)
- D (Download. Used in FT)
- H (Hard link creation. Used in FL)
- S (Symbolic link creation. Used in FL)

file-io-operation-name indicates a type of the following file I/O operations.

- FileRead (Finish of reading a file)
- FileWritten (Finish of wrting a file)
- FileDeleted (Finish of removing a file)
- DirectoryCreated (Finish of creating a directory)
- FileRenamed (Finish of renaming a file)
- LinkCreated (Finish of creating a hard link)
- SymbolicLinkCreated (Finish of creating a symbolic link)
- ListFilesRawFormat (To run ls or dir)

--

Output example:

```
2020/01/31 10:34:52.277120 127.0.0.1:51660 user[PAM] FileWritten[FT] /home/user/file_nodiskio_0
2020/01/31 10:34:52.277175 127.0.0.1:51660 user[PAM] FT U /home/user/file_nodiskio_0
2020/01/31 10:35:14.946750 127.0.0.1:51662 user[PAM] FileRead[FT] /home/user/file_nodiskio_0
2020/01/31 10:35:15.002770 127.0.0.1:51662 user[PAM] FT D /home/user/file_nodiskio_0
2020/01/31 10:35:30.002700 127.0.0.1:51662 user[PAM] FS /home/user/dir_sync/stat.log
2020/01/31 10:35:30.013558 127.0.0.1:51664 user[PAM] FileDeleted[FS] /home/user/dir_sync/stat.log
2020/01/31 10:35:47.713558 127.0.0.1:51664 user[PAM] FileDeleted[FR] /home/user/stat.3.log
2020/01/31 10:35:47.765413 127.0.0.1:51664 user[PAM] FR /home/user/stat.3.log
2020/01/31 10:38:45.686206 127.0.0.1:51670 user[PAM] DirectoryCreated[DC] /home/user/hmkdir13
2020/01/31 10:38:45.789370 127.0.0.1:51670 user[PAM] DC /home/user/hmkdir13
2020/01/31 10:39:22.411968 127.0.0.1:51674 user[PAM] FileRenamed[FM] /home/user/stat.log /home/user/stat2.log
2020/01/31 10:39:22.463710 127.0.0.1:51674 user[PAM] FM /home/user/stat.log /home/user/stat2.log
2020/01/31 10:40:00.087660 127.0.0.1:51678 user[PAM] SymbolicLinkCreated[FL] /home/user/stat2.log /home/user/stat.log
2020/01/31 10:40:00.165831 127.0.0.1:51678 user[PAM] FL S /home/user/stat2.log /home/user/stat.log
2020/01/31 10:40:13.693415 127.0.0.1:51680 user[PAM] LinkCreated[FL] /home/user/stat2.log /home/user/stat.h.log
2020/01/31 10:40:13.746160 127.0.0.1:51680 user[PAM] FL H /home/user/stat2.log /home/user/stat.h.log
2020/02/06 13:54:21.282066 127.0.0.1:50186 user[PAM] ListFilesRawFormat[L
```

```
R] /home/user/hmkdir4
2020/02/06 13:54:21.282104 127.0.0.1:50186 user[PAM] ListFilesRawFormat[L
R] /home/user/hmkdir5
--

--
Example1 :
FileOperationLog yes
Example2 :
FileOperationLog yes FileSize 10MB 10
Example3 :
FileOperationLog yes DatePattern yyyy-MM-dd
Example4 :
FileOperationLog yes FileSize 10MB 10 /var/tmp/hcpd.file.operation.log
--
```

2.1.105 CallbackScript

```
=====
Supported OS : Linux.x86
Format : CallbackScript <flag-available>[ <script-path>[ <data-store-path
>]]
-----
flag-available
Default : no
Range of Values : yes, no
-----
script-path
Default : none
Range of Values : path string of file system
-----
data-store-path
Default : none
Range of Values : path string of file system
=====
```

This option specifies a script (or a binary program) to run after application runs.

flag-available enables this option. 'yes' means calling the script.

script-path specifies a path of the script. When a tilde(~) is described at the head, it will be expanded to the home directory of a user who runs the application.

data-store-path specifies a path of saving data given at the run-time of the script which is information of parameters or a result of application running. When a tilde(~) is described at the head, it will be expanded to the home directory of a user who runs the application.

After all of processing on each application running is finished, hcpd runs the following command line.

```
=====
Command format : <script-path> <exit-code> <start-date-and-time> <end-date-and-time> <remote-ip> <username> <hcp-operation-name> <param-saved-path> <output-saved-path>
-----
```

script-path

Range of Values : path string of file system (already expanded of tilde)

exit-code

Range of Values : exit code

start-date-and-time

Range of Values : date and time in the format of YYYY/MM/DD hh:mm:ss

end-date-and-time

Range of Values : date and time in the format of YYYY/MM/DD hh:mm:ss

remote-ip

Range of Values : peer IP address and port number

username

Range of Values : user name and authentication method

hcp-operation-name

Range of Values : hcp, hrm, hcp-ls, hmkdir, hpwd, hmv, hln, transfer, remove, listraw, mkd, pwd, move, link, cwd

param-saved-path

Range of Values : path string of file system

output-saved-path

Range of Values : path string of file system

```
=====
script-path is a script path on hcpd.conf with expanding tilde(~).
```

exit-code is a reason code representing a result that application runs. The reason code is identical to a reason code recorded in the application statistics.

start-date-and-time is a date and time that application starts.

end-date-and-time is a date and time that application finishes.

hcp-operation-name indicates a type of the following applications (or operations of API).

- hcp (File transfer command)
- hrm (File removing command)
- hcp-ls (File listing command)
- hmkdir (Directory creation command)
- hpwd (Working directory printing command)
- hmv (File moving command)
- hln (Link creation command)
- transfer (API file transfer operation)
- remove (API file removing operation)
- listraw (API file listing operation)
- mkd (API directory creation operation)
- pwd (API working directory printing operation)
- move (API file moving operation)
- link (API link creation operation)

param-saved-path is a path of a file where information of input parameters is saved. The file includes options of the operation and path information from running result records (.hcp.out) the server recognizes.

--

Output example:

```
[user@localhost ~]$ cat .hcp/callback/hcp.cb.20200206_152252_468.13521.para
m
OPT copy_mode ALLCOPY
OPT overwrite_mode FORCE
OPT fail_action_mode HALT
OPT preserve_permission no
OPT recursive yes
OPT any_dirs no
OPT regex no
OPT verify_payload no
OPT copy_symlink no
OPT follow_symlink no
OPT no_copy_empty_file no
OPT no_copy_empty_dir no
OPT no_copy_dot_file no
OPT no_copy_dot_dir no
OPT copy_hidden no
OPT check_archive no
OPT resuming no
OPT no_app_io yes num_files 1 file_size 1024
```

```
OPT no_sess_io no
SRC /home/user
--
```

output-saved-path is a path of a file where a running result is saved. The file includes records representing a running result of each file.

```
--
Output example:
[user@localhost ~]$ cat .hcp/callback/hcp.cb.20200206_152252_468.13521.out
t
OK 0000 FT 00000001 /home/user/file_nodiskio_0
--
```

```
--
Example :
CallbackScript yes /var/tmp/hcp_callback.sh /var/tmp/hcp_callback
--
```

2.1.106 CallbackScriptHomeIsolation

```
=====
Supported OS : Linux.x86
Format : CallbackScriptHomeIsolation <flag-available>[ <logical-opt>]
-----
flag-available
Default : no
Range of Values : yes, no
-----
logical-opt
Default : none
Range of Values : logical
=====
```

This option prevents callback scripts out of user home directory from being called.

When logical-opt is set to 'logical', the validation of being out of it will be performed by a logical path (a path without dereference for symbolic links).

```
--
Example :
CallbackScriptHomeIsolation yes logical
--
```

2.1.107 CallbackScriptNoSymbolicLink

```
=====
Supported OS : Linux.x86
Format : CallbackScriptNoSymbolicLink <flag-available>
-----
```

flag-available

Default : no

Range of Values : yes, no

=====

This option prevents callback scripts as symbolic links from being called.

--

Example :

CallbackScriptNoSymbolicLink yes

--

2.1.108 DisableMemoryManager

=====

Supported OS : Linux.x86 / Windows

Format : DisableMemoryManager <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

This option disables memory management for file payloads splitted into data chunks to limit memory usage of the chunks over sessions.

If changing to 'no', hcpd will performs the limitation for download transfer of files on hcp and hsync. However, a problem blocking the transfer in some environment that might be from this feature was found. So please use this option only if you need.

--

Example :

DisableMemoryManager no

--

2.1.109 DiskBenchmarkPreAllocation

=====

Supported OS : Linux.x86

Format : DiskBenchmarkPreAllocation <how-to-pre-alloc>

how-to-pre-alloc

Default : none

Range of Values : none, native, posix

=====

This option specifies how to make pre-allocation of sotrage in some disk writing benchmarks performed by the run-host-benchmark option.

'none' disables the pre-allocation on the benchmarks.

'native' indicates making the pre-allocation by the platform dependent function, e.g., `fallocate` function on Linux.

'posix' indicates making the pre-allocation by the POSIX function as the `posix_fallocate` function.

This option will be used when performing benchmarks of Async I/O. Writing performance with the pre-allocation might be better than one without.

--

Example :

`DiskBenchmarkPreAllocation native`

--

2.1.110 `DiskBenchmarkPreAllocationSize`

```
=====
Supported OS : Linux.x86
Format : DiskBenchmarkPreAllocationSize <pre-allocation-size>
-----
pre-allocation-size
Default : 0
Range of Values : signed double-length integer
=====
```

This option specifies a unit size in bytes for the pre-allocation of storage described above.

When 0 or negative values are specified, the pre-allocation will be performed in a file size to write each benchmarks (one time allocation).

--

Example :

`DiskBenchmarkPreAllocationSize 1GB`

--

2.1.111 `DiskBenchmarkDirectAlignmentSize`

```
=====
Supported OS : Linux.x86
Format : DiskBenchmarkDirectAlignmentSize <alignment-size>
-----
alignment-size
Default : 0
Range of Values : unsigned double-length integer
=====
```

This option specified an alignment size in memory for writing and reading buffers used for some disk benchmarks with Direct I/O performed by the run-host-benchmark option.

Specification of 0 indicates to detect the size by querying to the system and use its result.

--

Example :

DiskBenchmarkDirectAlignmentSize 8KB

--

2.1.112 DiskBenchmarkAsyncNoWait (Reserved)

2.1.113 DiskBenchmarkAsyncMaxEvents

```
=====
Supported OS : Linux.x86
Format : DiskBenchmarkAsyncMaxEvents <num-max-events>
-----
num-max-events
Default : 16
Range of Values : signed integer
=====
```

This option specifies a maximum number of events processed at once in some disk benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

For example, when a result of writing performance is under an expected one with striped storages, the result might be improved increasing the maximum number.

--

Example :

DiskBenchmarkAsyncMaxEvents 32

--

2.1.114 DiskBenchmarkAsyncMaxGetEvents

```
=====
Supported OS : Linux.x86
Format : DiskBenchmarkAsyncMaxGetEvents <num-max-get-events>
-----
num-max-get-events
Default : 1
Range of Values : signed integer
=====
```

This option specified a maximum number of events to take its results at once in the benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

It is used for observing changes of performance characteristics increasing the number of results being taken at once.

```
--  
Example :  
DiskBenchmarkAsyncMaxGetEvents 4  
--
```

2.1.115 DiskBenchmarkAsyncRequestPoolSize

```
=====
Supported OS : Linux.x86
Format : DiskBenchmarkAsyncRequestPoolSize <pool-size>
-----
pool-size
Default : 32
Range of Values : unsigned integer
=====
```

This option specifies a size of a pool holding user buffers as I/O requests in some disk benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

```
--
Example :
DiskBenchmarkAsyncRequestPoolSize 64
--
```

2.1.116 DeepDiskBenchmarkFileSize

```
=====
Supported OS : Linux.x86
Format : DeepDiskBenchmarkFileSize <file-size>
-----
file-size
Default : 16GB
Range of Values : signed double-length integer
=====
```

This option specifies a file size used in some additional disk benchmarks performed by the run-host-benchmark option.

```
--
Example :
DeepDiskBenchmarkFileSize 32GB
--
```

2.1.117 DeepDiskBenchmarkFreeSpaceRequired

```
=====
Supported OS : Linux.x86
```

Format : DeepDiskBenchmarkFreeSpaceRequired <free-space-size>

free-space-size

Default : 32GB

Range of Values : unsigned double-length integer

=====

This option specifies a disk free space required in some additional disk benchmarks performed by the run-host-benchmark option.

--

Example :

DeepDiskBenchmarkFreeSpaceRequired 64GB

--

2.1.118 DeepDiskBenchmarkBlockSizes

=====

Supported OS : Linux.x86

Format : DeepDiskBenchmarkBlockSizes <block-size-set-desc>

block-size-set-desc

Default : 16KB 32KB 64KB 128KB 256KB 512KB 1MB 2MB

Range of Values : a set of block sizes separated with white spaces

=====

This option specifies a set of block sizes used in some additional disk benchmarks performed by the run-host-benchmark option.

--

Example :

DeepDiskBenchmarkBlockSizes 64KB 256KB 512KB 1MB

--

2.1.119 MemoryTransferConcurrency

=====

Supported OS : Linux.x86 / Windows

Format : MemoryTransferConcurrency <num-concur> <wait-type> <busy-sleep-n sec>

num-concur

Default : auto (smaller value of physical-CPU/2 or 16)

Range of Values : unsigned integer

wait-type

Default : cond

Range of Values : cond, busy

busy-sleep-nsec

Default : 1

Range of Values : unsigned integer

=====

When you use -n option on the hcp command which starts the command on memory-to-memory transfer mode, this option configures how to copy memory data of file payloads in concurrent way at the sender side.

num-concur specifies a number of concurrent copies. 1 indicates the standar memory copy by memcpy without concurrency.

wait-type specifies a waiting method on memory copy threads in its idling state. cond is to perform a conditinal wait on that idling state and busy is to perform a busy wait on it. When busy is set, CPU usage might be up to a multiplication of the number of CPUs and 100%.

busy-sleep-nsec specifies a waiting time in nano seconds on the busy wait.

This options is defined for a performance tuning to remove performance limitation by a single threaded memory copy on 100Gbps network environment.

--

Example :

MemoryTransferConcurrency 1 cond 1 # To disable

MemoryTransferConcurrency 12 busy 1 # Busy wait, 4 concurrent and wait in 1 nano seconds

--

2.1.120 MaxReadRate

=====

Supported OS : Linux.x86 / Windows

Format : MaxReadRate <read-rate>

read-rate

Default : 10Ebit (Unlimited)

Range of Values : unsigned double-length integer (up to 10Ebit)

=====

This option specifies limitation of reading data from files on file transfer. This will be applied to each session which performs the file transfer. It is recognized as unlimited when the value is the maximum value in bps or over it.

In some environment, long time running of reading and writing might make overheat on SSDs (especially the writing side). So this option is useful for avoiding it.

--

Example :

MaxReadRate 10Gbit

--

The old name of 'MaxReadRatePerConnection' is available.

2.1.121 MaxWriteRate

```
=====
Supported OS : Linux.x86 / Windows
Format : MaxWriteRate <write-rate>
-----
write-rate
Default : 10Ebit (Unlimited)
Range of Values : unsigned double-length integer (up to 10Ebit)
=====
```

This option specifies limitation of writing data to files on file transfer. This will be applied to each session which performs the file transfer. It is recognized as unlimited when the value is the maximum value in bps or over it.

In some environment, long time running of reading and writing might make overheat on SSDs (especially the writing side). So this option is useful for avoiding it.

--

Example :

MaxWriteRate 10Gbit

--

The old name of 'MaxWriteRatePerConnection' is available.

2.1.122 EnsureDestinationInFileTransfer

```
=====
Supported OS : Linux.x86 / Windows
Format : EnsureDestinationInFileTransfer <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When the destination directory doesn't exist during file transfers, how to control the file transfer, whether a new directory is created is set. This option is fixed to "no" from the software version 1.1.0.

--

Example :

EnsureDestinationInFileTransfer no

--

2.1.123 StatLogPerUserInPrivilegeSeparation

```
=====
Supported OS : Linux.x86 / Windows
Format : StatLogPerUserInPrivilegeSeparation <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

In the case of the privilege separation, whether to record the statistics log for each user, is chosen.

```
--
Example :
StatLogPerUserInPrivilegeSeparation yes
--
```

2.1.124 NoSupplementalGroupInPrivilegeSeparation

```
=====
Supported OS : Linux.x86
Format : NoSupplementalGroupInPrivilegeSeparation <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

This option disables supplemental groups on the privilege separation.

```
--
Example :
NoSupplementalGroupInPrivilegeSeparation yes
--
```

2.1.125 ApplicationStatLogSecurityEx

```
=====
Supported OS: Linux.x86 / Windows
Format : ApplicationStatLogSecurityEx <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

Whether to output the detailed information on the security in the application statistics log is set.

```
--  
Example :  
ApplicationStatLogSecurityEx no  
--
```

2.1.126 GetGrRMaxBufferSize

```
=====
Supported OS : Linux.x86
Format : GetGrRMaxBufferSize <max-buf-size>
-----
max-buf-size
Default : 512KB
Range of Values : unsigned integer
=====
```

This option changes a maximum buffer size that will be used for queries of group information that require larger buffers than the default buffer of 8KB, e.g. having description of many users on that definition in /etc/group.

In usual cases, you do not have to change this option. Please try to do when some errors due to the buffer size problem happen.

```
--
Example :
GetGrRMaxBufferSize 1MB
--
```

2.1.127 GetPwRMaxBufferSize

```
=====
Supported OS : Linux.x86
Format : GetPwRMaxBufferSize <max-buf-size>
-----
max-buf-size
Default : 64KB
Range of Values : unsigned integer
=====
```

This option changes a maximum buffer size that will be used for queries of user information that require larger buffers than the default buffer of 8KB.

In usual cases, you do not have to change this option. Please try to do when some errors due to the buffer size problem happen.

```
--
Example :
GetPwRMaxBufferSize 128KB
--
```


2.2 Client common command configuration list.

Common client commands available are as follows.

setting item	explanation
ProtocolVersion	protocol version (fixed to 2)
RequireServerCertificateSecurity	server certificate security request
RejectFallbackServerCertificateSecurity	fallback server certificate security rejection
IgnoreCertificateCNInvalid	ignore common name
IgnoreCertificateDateInvalid	ignore certificate expiration
IgnoreUnknownCA	ignore Unknown CA
IgnoreRevocation	ignore revocation
WSSIgnoreCertificateCNInvalid	No validation for common names(WebSocket)
WSSIgnoreCertificateDateInvalid	No validation for certificate expires(WebSocket)
WSSIgnoreUnknownCA	No validation for CA and intermediates(WebSocket)
WSSIgnoreRevocation	No validation for revocation(WebSocket)
WSSOptions	WSS options
WSSCipherSuites	WSS TLS 1.3 Cipher Suites options
WSSCipherList	WSS TLS 1.2 or earlier Cipher Suites options
CACertificateFile	CA certification file
CACertificatePath	CA certification path (reserved)
CARevocationFile	CRL revocation file
CARevocationPath	CRL revocation path (reserved)
OCSPRevocationEnabled	OCSP (online Certificate revocation check)function
StrictHostKeyChecking	server host key acceptance policy
LocalPasswordAuthentication	LPA authentication
PAMAuthentication	PAM authentication
PubkeyAuthentication	public key authentication
WinLogonUserAuthentication	Windows authentication
NumberOfPasswordPrompts	number of prompts to enter password

IdentitySearchDir	private key search directory
IdentityFile	private key file
AcceptableCryptMethod	valid cryptographic method
AcceptableDigestMethod	valid digest method
DisableDataIntegrityChecking	disable data integrity check
AcceptDataIntegrityCheckingOnRejection	disabled data integrity check rejection acceptance
TransportCharEncoding	transport character encoding
HostEncoding	host character encoding
CompressLevel	compress level
HeaderCompress	header compression
ContentCompress	content compression
MaxConcurrentThread	max current thread (Linux)
MaxReceiveFileSize	max receive file size
MaxSendFileSize	max send file size
MaxRequestFileEntryAtOnce	max file entry request
MaxBufferSize	max payload memory buffer
MaxReceiveRate	max receive rate (per session)
MaxSendRate	max send rate (per session)
MaxConnectionReceiveRate	max receive rate (per connection)
MaxConnectionSendRate	max send rate (per connection)
InitHeaderBlockSize	initial header block size
InitContentBlockSize	initial content block size
MaxHeaderBlockSize	max header block size
MaxContentBlockSize	max content block size
FileLock	file lock
FileLockTrials	file rock retry number
FileLockTrialInterval	file rock retry interval (sec)
TransportTimeout	transport timeout
DiagnosticLog	log settings(ApplicationLog as old one)
DiagnosticLogLevel	application log level
ApplicationStatLog	application statistics
TransportStatLog	transport statistics

UDPTransportExtensionBufferSize	HpFP transport buffer size extension
TCPTransportSocketSendBuffer	TCP sending buffer
PubkeyAuthenticationPrior	public key authentication priority setting
ApplicationStatLogSecurityEx	detailed security information output setting for application statistics logs
DiskBenchmarkPreAllocation	how to make pre-allocation in disk benchmark
DiskBenchmarkPreAllocationSize	a unit size for the pre-allocation
DiskBenchmarkDirectAlignmentSize	Direct I/O benchmark, alignment size specification
DiskBenchmarkAsyncNoWait	Async I/O benchmark, NO_WAIT(reserved)
DiskBenchmarkAsyncMaxEvents	Async I/O benchmark, maximum number of I/O events at once
DiskBenchmarkAsyncMaxGetEvents	Async I/O benchmark, maximum number of taking event results at once
DiskBenchmarkAsyncRequestPoolSize	Async I/O benchmark, a size of pool holding request buffers
DeepDiskBenchmarkFileSize	file size on additional disk benchmarks
DeepDiskBenchmarkFreeSpaceRequired	required free space on the benchmarks
DeepDiskBenchmarkBlockSizes	a set of block sizes on the benchmarks

2.2.1 RequireServerCertificateSecurity

```
=====
Supported OS : Linux / Windows / Mac
Format : RequireServerCertificateSecurity <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

Whether the security communication by the server certificate security function is required or not is set. When “yes”, but this function isn’t enabled on the host, the connection is denied.

```
--
Example :
RequireServerCertificateSecurity no
--
```

2.2.2 RejectFallbackServerCertificateSecurity

```
=====
Supported OS : Linux / Windows / Mac
Format : RejectFallbackServerCertificateSecurity <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When the security communication by the server certificate security function can not be established, the fallback to the unsafe communication is rejected.

```
--
Example :
RejectFallbackServerCertificateSecurity no
--
```

2.2.3 IgnoreCertificateCNInvalid

```
=====
Supported OS : Linux / Windows / Mac
Format : IgnoreCertificateCNInvalid <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

It is set to ignore identifying the server certificate common name. When “yes”, identification of the server certificate common name with an IP address or a FQDN of the server is omitted.

```
--
Example :
IgnoreCertificateCNInvalid yes
--
```

2.2.4 IgnoreCertificateDateInvalid

```
=====
Supported OS : Linux / Windows / Mac
Format : IgnoreCertificateDateInvalid <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

It is set to ignore the check of the server certificate expiration. When “yes”, the expiration of the server certificate is not checked.

```
--  
Example :  
IgnoreCertificateDateInvalid yes  
--
```

2.2.5 IgnoreUnknownCA

```
=====
Supported OS : Linux / Windows / Mac
Format : IgnoreUnknownCA <flag-available>
```

```
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

It is set to ignore the check of CA certificates. When “yes”, the intermediate certificate and the root certificate of the server certificate are not checked.

```
--  
Example :  
IgnoreUnknownCA yes  
--
```

2.2.6 IgnoreRevocation

```
=====
Supported OS : Linux / Windows / Mac
Format : IgnoreRevocation <flag-available>
```

```
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

It is set to ignore the certificate revocation check. When “yes”, the certificate revocation is not checked.

```
--  
Example :  
IgnoreRevocation yes  
--
```

2.2.7 WSSIgnoreCertificateCNInvalid

```
=====
Supported OS : Linux / Windows / Mac
```

Format : WSSIgnoreCertificateCNInvalid <flag-available>

flag-available

Default : no

Range of Values : yes, no
=====

This option disables validation for common names of server certificates that are sent to the client on communication via WebSocket with SSL/TLS. When yes is set, the WebSocket function dose not make validation to confirm if the common name on the certificate received is identical to an FQDN or IP address specified as the server.

--

Example :

WSSIgnoreCertificateCNInvalid yes

--

2.2.8 WSSIgnoreCertificateDateInvalid

=====

Supported OS : Linux / Windows / Mac

Format : WSSIgnoreCertificateDateInvalid <flag-available>

flag-available

Default : no

Range of Values : yes, no
=====

This option disables validation for expires of server certificates that are sent to the client on communication via WebSocket with SSL/TLS. When yes is set, the WebSocket function dose not make validation to confirm if NotBefore and NotAfter on the certificate received meet the current date and time.

--

Example :

WSSIgnoreCertificateDateInvalid yes

--

2.2.9 WSSIgnoreUnknownCA

=====

Supported OS : Linux / Windows / Mac

Format : WSSIgnoreUnknownCA <flag-available>

flag-available

Default : no

Range of Values : yes, no
=====

This options disables validation for CA certificates bound to server certificate that are sent to the client on communication via WebSocket with SSL/TLS. When yes is set, the WebSocket function dose not make validation to confirm if CA root certificate and intermediate certificates bound to the server certificates are available.

--

Example :

WSSIgnoreUnknownCA yes

--

2.2.10 WSSIgnoreRevocation (reserved)

2.2.11 WSSOptions

=====

Supported OS : Linux / Windows / Mac

Format : WSSOptions <opt_value>

opt_value

Format : (NONE | <openssl_opt_values>)

Default : NONE

Range of Values : list of SSL/TLS option names defined by OpenSSL

=====

This options specifies Cipher Suites options of OpenSSL that will be used on SSL/TLS communication. Please use names described in the following URL.

https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_options.html

SSL_CTX_set_options

--

Example :

WSSOptions SSL_OP_NO_COMPRESSION:SSL_OP_NO_SSLv3

--

2.2.12 WSSCipherSuites

=====

Supported OS : Linux / Windows / Mac

Format : WSSCipherSuites <cs_value>

cs_value

Format : (NONE | <openssl_cipher_suite_values>)

Default : NONE

Range of Values : list of Cipher Suites parameters defined by OpenSSL

=====

This options specifie Cipher Suites parameters of OpenSSL that will be used on TLS v1.3 communication. Please use names described in the following URL.

<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>
ciphers

Ciphte Suite names defined by "TLS v1.3 cipher suites"

--

Example :

WSSCipherSuites TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256

--

2.2.13 WSSCipherList

```
=====
Supported OS : Linux / Windows / Mac
Format : WSSCipherList <clist_value>
-----
clist_value
Format : ( NONE | <openssl_cipher_list> )
Default : NONE
Range of Values : Cipher List parameters defined by OpenSSL
=====
```

This option specifies Cipher List parameters of OpenSSL that will be used on SSL/TLS communication under TLS 1.2. Please use names described in the following URL.

<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>
ciphers

Cipher List in a format defined by "CIPHER LIST FORMAT2 and "CIPHER STRINGS".

--

Example :

WSSCipherList RC4-MD5:RC4-SHA:AES128-SHA:AES256-SHA:HIGH:!DSS:!aNULL

--

2.2.14 CACertificateFile

```
=====
Supported OS : Linux / Windows / Mac
Format : CACertificateFile <file-path>
-----
file-path
Default :
  /etc/hcp/cacert.pem (Linux)
  C:/ProgramData/Clealink/HCP Tools/cacert.pem (Windows)
  /usr/local/etc/hcp/cacert.pem (Mac)
```


Range of Values : path string of file system

The file path of the CA certificate for the server certificate is specified.

--

Example :

CACertificateFile /etc/hcp/cacert.pem

--

The PEM format certificates are supported.

2.2.15 CACertificatePath (reserved)

Supported OS : Linux / Windows / Mac

Format : CACertificatePath <dir-path>

dir-path

Default : yes

/etc/ssl (Linux)

C:/ProgramData/Clealink/HCP Tools/ssl (Windows)

/usr/local/etc/ssl (Mac)

Range of Values : path string of file system

The directory path of the CA certificate for the server certificate is specified.

--

Example :

CACertificatePath /etc/ssl

--

The PEM format certificates are supported.

2.2.16 CARevocationFile

Supported OS : Linux / Windows / Mac

Format : CARevocationFile <file-path>

file-path

Default : yes

/etc/hcp/crl.pem (Linux)

C:/ProgramData/Clealink/HCP Tools/crl.pem (Windows)

/usr/local/etc/hcp/crl.pem (Mac)

Range of Values : path string of file system

The file where the certificate revocation list (CRL) is stored for the server certificate is specified.

```
--  
Example :  
CARevocationFile /etc/hcp/crl.pem  
--
```

The PEM format certificate revocation list (CRL) is supported.

2.2.17 CARevocationPath (reserved)

```
=====
Supported OS : Linux / Windows / Mac
Format : CArrevocationPath <dir-path>
-----
dir-path
Default : yes
    /etc/ssl (Linux)
    C:/ProgramData/Clealink/HCP Tools/ssl (Windows)
    /usr/local/etc/ssl (Mac)
Range of Values : path string of file system
=====
```

The directory where the certificate revocation list (CRL) is stored for the server certificate is specified.

```
--
Example :
CARevocationPath /etc/ssl
--
```

The PEM format certificate revocation list (CRL) is supported.

2.2.18 WSSCACertificateFile

```
=====
Supported OS : Linux / Windows / Mac
Format : WSSCACertificateFile <file-path>
-----
file-path
Default : none
Range of Values : path string of file system
=====
```

This option specifies a path of a file that includes CA certificates provided for validation of server certificates received on the WebSocket SSL/TLS communication. When this is not set, the WebSocket function will use the default CA certificates it detects.

```
--  
Example :  
WSSCACertificateFile /etc/hcp/cacert.pem  
--
```

2.2.19 OCSPRevocationEnabled

```
=====
```

Supported OS : Linux / Windows / Mac
Format : OCSPRevocationEnabled <flag-available>

flag-available
Default : yes
Range of Values : yes, no
=====

It sets OCSP (Online Certificate Status Protocol) for the server certificate identification. When “yes”, it is enable.

```
--  
Example :  
OCSPRevocationEnabled no  
--
```

2.2.20 StrictHostKeyChecking

```
=====
```

Supported OS : Linux / Windows / Mac
Format : StrictHostKeyChecking <switch>

switch
Default : ask
Range of Values : ask, yes, no
=====

The policy to accept the server host is set here. When “ask”, whether to accept unknown keys is confirmed. When “yes”, it stops authenticating. When “no”, continue authenticating without confirming.

```
--  
Example :  
StrictHostKeyChecking no  
--
```

2.2.21 LocalPasswordAuthentication

```
=====
```

Supported OS : Linux / Windows / Mac
Format : LocalPasswordAuthentication <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

LPA authentication is set. When “no”, even though the server requests the authentication, LPA authentication is not executed.

--

Example :

LocalPasswordAuthentication no

--

2.2.22 PAMAuthentication

=====

Supported OS : Linux / Windows / Mac

Format : PAMAuthentication <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

PAM authentication is set. When “no”, even though the server requests the authentication, PAM authentication is not executed.

--

Example :

PAMAuthentication no

--

2.2.23 PubkeyAuthentication

=====

Supported OS : Linux / Windows / Mac

Format : PubkeyAuthentication <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

Public key authentication is set. When “no”, even though the server requests the authentication, it is not executed.

--

Example :

PubkeyAuthentication no

--

2.2.24 WinLogonUserAuthentication

```
=====
Supported OS : Linux / Windows / Mac
Format : WinLogonUserAuthentication <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

Windows authentication is set. When “no”, even though the server requests the authentication, Windows authentication is not executed.

```
--
Example :
WinLogonUserAuthentication no
--
```

2.2.25 NumberOfPasswordPrompts

```
=====
Supported OS : Linux / Windows / Mac
Format : NumberOfPasswordPrompts <num-prompts>
-----
num-prompts
Default : 3
Range of Values : signed integer
=====
```

This option specifies the number of prompts to enter a password (passphrase) each authentication when performing password authentications of PAM, WLU or LPA or decryption of a private key. When all tries are not successful up to the number of prompts, then the next one goes on.

```
--
Example :
NumberOfPasswordPrompts 2
--
```

2.2.26 IdentitySearchDir

```
=====
Supported OS : Linux / Windows / Mac
Format : IdentitySearchDir <flag-available>
-----
flag-available
Default :
    /etc/hcp/keys (Linux)
    C:/ProgramData/Clealink/HCP Tools/keys (Windows)
```

Bytix Archaea tools Command Reference

/usr/local/etc/hcp/keys (Mac)
Range of Values : path string of file system
=====

The search directory is configured in order to identify the user private key for public key authentication.

--
Example :
IdentitySearchDir /etc/hcp/keys
--

The following file name in the specified directory is searched as a file which stores the private key.

<user name>.key

This username is the local computer username, not the username of the destination server (that is specified by -u option or used in the login prompt.) In the case that the local computer username is different from the server username, make sure to set the local username.

On the Linux platform, some files having access permissions on its Group and Other will be skipped with displayed warnings.

When a file with the same name as the user name and the following extensions exists in the same directory as the one of the private key, the file is regarded as the client certificate and is authenticated.

- crt
- cer

This software supports the following formats of private keys.

- PEM
- OpenSSH v1
- PuTTY v2/v3

And it supports PEM formatted certificates.

About key algorithms, the following algorithms are supported.

- RSA (1024bits - 4096bits)
- ECDSA nistp256, nistp384, nistp521
- Ed25519

When key agents like ssh-agent and pageant are working on client hosts, public key authentication without passphrases will be performed for a key from keys that are detected by this configuration and in the following format.

- OpenSSH v1 formatted private key
- PuTTY v2/v3 formatted private key

Clients use ssh-agent on Linux/macOS and pageant on Windows (ssh-agent is not supported on Windows).

The old name of 'PrivateKeySearchDir' is available.

2.2.27 IdentityFile

```
=====
Supported OS : Linux / Windows / Mac
Format : IdentityFile <file-path>
-----
file-path
Default :
(Linux / Mac)
~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.ssh/id_ed25519
~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519
(Windows)
~/_hcp/id_rsa ~/_hcp/id_ecdsa ~/_hcp/id_ed25519
Range of Values : the single file path which includes the user directory
with a tilde (~)
=====
```

The path of the file with the key in the user home directory is configured in order to identify the user private key for RSA authentication.

```
--
Example :
IdentityFile ~/.hcp/id_rsa
--
```

On the Linux platform, some files having access permissions on its Group and Other will be skipped with displayed warnings.

When the specified file and the same name file with the following suffixes both exist, it is regarded as the client certificate and authenticated.

- crt
- cer

This software supports the following formats of private keys.

- PEM

Bytix Archaea tools Command Reference

- OpenSSH v1
- PuTTY v2/v3

And it supports PEM formatted certificates.

About key algorithms, the following algorithms are supported.

- RSA (1024bits - 4096bits)
- ECDSA nistp256, nistp384, nistp521
- Ed25519

TOKENS of %2, %d, %i, %r and %u is available defined under the following ssh_config.

https://man7.org/linux/man-pages/man5/ssh_config.5.html
TOKENS - IdentityFile

Multiple entries are available with multiple configuration entries in specifying a single path each entry.

```
IdentityFile ~/.hcp/id_mykey1
IdentityFile ~/.hcp/id_mykey2
IdentityFile ~/.hcp/id_mykey3
```

You cannot multiple paths in the single configuration entry.

When key agents like ssh-agent and pageant are working on client hosts, public key authentication without passphrases will be performed for a key from keys that are detected by this configuration and in the following format.

- OpenSSH v1 formatted private key
- PuTTY v2/v3 formatted private key

Clients use ssh-agent on Linux/macOS and pageant on Windows (ssh-agent is not supported on Windows).

The old name of 'PrivateKeyFile' is available.

2.2.28 AcceptableCryptMethod

```
=====
Supported OS : Linux / Windows / Mac
Format : AcceptableCryptMethod <method-names>
-----
method-names
Format : <method-name>[ ...]
Default : AES256/GCM AES256/CTR/VMAC AES256/CBC AES128/CBC
-----
method-name
Range of Values : PLAIN, AES128/CBC, AES192/CBC, AES256/CBC, AES128/CBC/H
```



```
MAC,  
AES192/CBC/HMAC, AES256/CBC/HMAC, AES128/CBC/VMAC, AES192/CBC/VMAC,  
AES256/CBC/VMAC, AES128/CBC/VMAC64, AES192/CBC/VMAC64, AES256/CBC/VMAC64,  
AES128/CTR/HMAC, AES192/CTR/HMAC, AES256/CTR/HMAC, AES128/CTR/VMAC,  
AES192/CTR/VMAC, AES256/CTR/VMAC, AES128/CTR/VMAC64, AES192/CTR/VMAC64,  
AES256/CTR/VMAC64, AES128/GCM, AES192/GCM, AES256/GCM  
=====
```

The cryptographic algorithm is configured.

When specified AES128/CBC, it is interpreted as AES128/CBC/HMAC (They are the same algorithm. AES192/CBC and AES256/CBC are as well).

When communicating with a host with versions (1.2.5 or earlier) that do not support the new algorithms, such as CTR/GCM mode and VMAC mode, these new algorithms that don't match the other host are ignored in the connection negotiation. However, still, the communications don't go to errors.

CTR/VMAC or GCM are recommended on network over 1Gbps, e.g. AES256/GCM, AES256/CTR/VMAC. Encrypted communication using CBC or HMAC, e.g. AES256/CTR/HMAC, AES256/CBC/HMAC, might make a bottle neck in performance on network over 1Gbps generally. VMAC64 checks data integrity with 64 bit, less than 128 bit in VMAC mode, which leads to better performance but less secured data integrity.

```
--  
Example :  
AcceptableCryptMethod AES256/CBC PLAIN  
--
```

It is used to encrypt the messages communicated with the server. The algorithm is chosen to match the server configuration.

2.2.29 AcceptableDigestMethod

```
=====  
Supported OS : Linux / Windows / Mac  
Format : AcceptableDigestMethod <method-names>  
-----  
method-names  
Format : <method-name>[ ...]  
Default : XXH3 SHA256 SHA160  
-----  
method-name  
Range of Values : NONE, SHA160, SHA224, SHA256, SHA384, SHA512, MD5, MM32,  
MM128,  
XXH3, XXH128, XXH64, XXH32  
=====
```

The digest algorithm is configured.

```
--  
Example :  
AcceptableDigestMethod SHA256 SHA160 NONE  
--
```

It is used to verify the messages, files, and data blocks communicated with the server. The algorithm is chosen to match the server configuration.

In the case of encryption communications using HMAC like AES256/CBC/HMAC, the algorithms (MD5, MM32, MM128, XXH3, XXH128, XXH64, XXH32) other than the security digest algorithms are regarded as nothing configured.

MM32 and MM128 are discarded (, but its definition is kept for configuration compatibility). Please use XXH3 instead.

2.2.30 DisableDataIntegrityChecking

```
=====
Supported OS : Linux / Windows / Mac
Format : DisableDataIntegrityChecking <flag-available>
-----
flag-available
Default : no
Range of Values : yes, no
=====
```

This setting specifies whether to request the server to ignore data integrity checking by MAC in encrypted communications with the server.

When “yes”, it allows to transmit encrypted communication without data integrity checking as long as the server permits it. In the case that the server denies, it follows the setting of “AcceptDataIntegrityCheckingOnRejection” below.

In normal use, “no” (default) is recommended. Note that data integrity checking is not executed in the setting “yes”, which is supposed to be set only to improve the encrypted communication performance.

```
--  
Example :  
DisableDataIntegrityChecking yes  
--
```

2.2.31 AcceptDataIntegrityCheckingOnRejection

```
=====
Supported OS : Linux / Windows / Mac
Format : AcceptDataIntegrityCheckingOnRejection <flag-available>
```

```
-----  
flag-available  
Default : yes  
Range of Values : yes, no  
=====
```

This setting specifies whether to continue transmitting when the server denies the request to ignore data integrity checking by MAC in encrypted communications.

When “yes”, it continues transmitting with data integrity checking, while in “no”, it stops transmitting and quit the application.

```
--  
Example :  
AcceptDataIntegrityCheckingOnRejection no  
--
```

2.2.32 TransportCharEncoding

```
=====
```

Supported OS : Linux / Windows / Mac
Format : TransportCharEncoding <encodings>

```
-----  
encodings  
Format : <encoding>[ ...]  
Default : UTF8  
-----
```

```
encoding  
Range of Values : US-ASCII, UTF8, UTF16, UTF32  
=====
```

The string encoding method used in the transport is configured.

```
--  
Example :  
TransportCharEncoding UTF8 UTF16 US-ASCII  
--
```

It is used to exchange strings with the server, such as file path. The encoding is chosen to match the server configuration.

2.2.33 HostEncoding

```
=====
```

Supported OS : Linux / Windows / Mac
Format : HostEncoding <encoding>

```
-----  
encoding  
Default :  
    UTF-8 (Linux / Mac)
```

CP932 (Windows)

Range of Values : encoding name supported by system and encoding conversion library (platform-dependent).

The string encoding for the host is configured.

--

Example :

HostEncoding EUC-JP

--

2.2.34 CompressLevel

Supported OS : Linux / Windows / Mac

Format : CompressLevel <compress-level>

compress-level

Default : -1

Range of Values : -1, 0 - 9

The compression level of the transmission messages is set.

--

Example :

CompressLevel 9

--

When -1 is set, the compression level 6 is chosen.

When 0 is set, no compression will be performed.

2.2.35 HeaderCompress

Supported OS : Linux / Windows / Mac

Format : HeaderCompress <flag-available>

flag-available

Default : yes

Range of Values : yes, no

The compression of the header information such as the file request is configured.

--

Example :

HeaderCompress no

--

2.2.36 ContentCompress

```
=====
Supported OS : Linux / Windows / Mac
Format : ContentCompress <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

The compression of the data of files is configured.

--

Example :

ContentCompress no

--

2.2.37 MaxConcurrentThread

```
=====
Supported OS : Linux
Format : MaxConcurrentThread <max-threads>
-----
max-threads
Default : 0
Range of Values : signed integer
=====
```

The maximum number of threads is configured.

2.2.38 MaxReceiveFileSize

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxReceiveFileSize <file-size>
-----
file-size
Default : 8EB - 1B (Unlimited. The maximum value of signed double-length
integer)
Range of Values : signed double-length integer
=====
```

The maximum file size allowed to receive is set.

--

Example :

MaxReceiveFileSize 1GB

--

2.2.39 MaxSendFileSize

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxSendFileSize <file-size>
-----
file-size
Default : 8EB - 1B (Unlimited. The maximum value of signed double-length
integer)
Range of Values : signed double-length integer
=====
```

The maximum file size allowed to send is set.

--

Example :

MaxSendFileSize 1GB

--

2.2.40 MaxRequestFileEntryAtOnce

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxRequestFileEntryAtOnce <max-file-req-at-once>
-----
max-file-req-at-once
Default : 50
Range of Values : signed integer
=====
```

The maximum number allowed to send the file requests simultaneously is set.

--

Example :

MaxRequestFileEntryAtOnce 1000

--

2.2.41 MaxBufferSize

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxBufferSize <max-buf-size>
-----
max-buf-size
Default : 1GB
Range of Values : unsigned double-length integer
=====
```

The maximum memory buffer size allowed to process data is set.

```
--  
Example :  
MaxBufferSize 1GB  
--
```

2.2.42 MaxReceiveRate

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxReceiveRate <bandwidth>
-----
bandwidth
Default : 100Gbit
Range of Values : unsigned double-length integer
=====
```

The shaping of receiving bandwidth on the transport by each session is set.

```
--
Example :
MaxReceiveRate 1Gbit
--
```

2.2.43 MaxSendRate

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxSendRate <bandwidth>
-----
bandwidth
Default : 100Gbit
Range of Values : unsigned double-length integer
=====
```

The shaping of sending bandwidth on the transport by each session is set.

```
--
Example :
MaxSendRate 1Gbit
--
```

2.2.44 MaxConnectionReceiveRate

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxConnectionReceiveRate <bandwidth>
-----
bandwidth
Default : 100Gbit
```

Range of Values : unsigned double-length integer

The shaping of receiving bandwidth on the transport by each connection is set.

--

Example :

MaxConnectionReceiveRate 1Gbit

--

2.2.45 MaxConnectionSendRate

Supported OS : Linux / Windows / Mac

Format : MaxConnectionSendRate <bandwidth>

bandwidth

Default : 100Gbit

Range of Values : unsigned double-length integer

The shaping of sending bandwidth on the transport by each connection is set.

--

Example :

MaxConnectionSendRate 1Gbit

--

2.2.46 InitHeaderBlockSize

Supported OS : Linux / Windows / Mac

Format : InitHeaderBlockSize <block-size>

block-size

Default : 50KB

Range of Values : unsigned double-length integer

The initial header block size is set.

--

Example :

InitHeaderBlockSize 10KB

--

The maximum size allowed to create the header block including several messages such as file requests is set. This option is supposed to apply right after starting the communication.

2.2.47 InitContentSize

```
=====
Supported OS : Linux / Windows / Mac
Format : InitContentSize <block-size>
-----
block-size
Default : 1MB
Range of Values : unsigned double-length integer
=====
```

The initial content block size is set.

```
--
Example :
InitContentSize 2MB
--
```

The maximum size allowed to create the content block including several data of files is set. This option is supposed to apply right after starting the communication.

2.2.48 MaxHeaderBlockSize

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxHeaderBlockSize <block-size>
-----
block-size
Default : 50MB
Range of Values : unsigned double-length integer
=====
```

The maximum extension size of the header block is set.

```
--
Example :
MaxHeaderBlockSize 100KB
--
```

When the transmission starts, the changeable header block size is increased or decreased by sensing the consumed bandwidth. This option gives the max value of the header block size to increase.

2.2.49 MaxContentSize

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxContentSize <block-size>
-----
block-size
```

Default : 1MB
Range of Values : unsigned double-length integer
=====

The maximum extension size of the content block is set.

When the performance hits a peak in the environment over 10Gbps and others, changing this value along with “InitContentBlockSize” may improve performance.

--
Example :
MaxContentBlockSize 4MB
--

When the transmission starts, the changeable content block size is increased or decreased by sensing the consumed bandwidth. This option gives the max value of the content block size to increase.

2.2.50 FileLock

Refer to the hcpd configurations.

2.2.51 FileLockTrials

Refer to the hcpd configurations.

2.2.52 FileLockTrialInterval

Refer to the hcpd configurations.

2.2.53 TransportTimeout

Refer to the hcpd configurations.

2.2.54 DiagnosticLog

=====

Supported OS : Linux / Windows / Mac
Format : DiagnosticLog <log-level>[<flag-available>][<log-rotation-conf>][<log-path>]

log-level
Default : INFO
Range of Values : EMERG, ALERT, CRIT, ERR, WARNING, INFO, DEBUG

flag-available
Default : yes
Range of Values : yes, no

Bytix Archaea tools Command Reference

```
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
-----
log-path
Default : none
Range of Values : path string of file system
=====
<pre>
```

p. The application diagnostic log settings. The log includes some details of errors for trouble shooting.

p. log-level specifies the log level.

p. With flag-available yes, the log is output.

p. log-rotation-conf specifies the log rotation. It works in the same way as the rotation behavior set in "SystemLog", although it doesn't rotate periodically.

p. log-path specifies the log path. When it is set with the command line parameter "-l" simultaneously, the command line parameter setting is applied.

```
<pre>
--
Example1 :
DiagnosticLog WARNING FileSize 10MB 10
Example2 :
DiagnosticLog WARNING DatePattern yyyy-MM-dd
Example3:
DiagnosticLog WARNING // the same as "DiagnosticLogLevel"
--
```

The old name of 'ApplicationLog' is available.

2.2.55 DiagnosticLogLevel

```
=====
Supported OS : Linux / Windows / Mac
Format : DiagnosticLogLevel <log-level>
-----
log-level
Default : INFO
Range of Values : EMERG, ALERT, CRIT, ERR, WARNING, INFO, DEBUG
=====
```

The application log level is set.

When it was set along with "DiagnosticLog", only the log level is overwritten.

```
--
Example :
DiagnosticLogLevel WARNING
--
```

The old name of 'ApplicationLogLevel' is available.

2.2.56 ApplicationStatLog

```
=====
Supported OS : Linux / Windows / Mac
Format : ApplicationStatLog <flag-available>[ <log-rotation-conf>]
-----
flag-available
Default : yes
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
=====
```

The configuration on the application statistics is set.

When “yes” in “flag-available”, the application statistics information is output.

log-rotation-conf specifies the log rotation. It works in the same way as the rotation behavior set in “ApplicationStatLog” on hcpd.

```
--
Example1 :
ApplicationStatLog no
Example2 :
ApplicationStatLog yes FileSize 10MB 10
Example3 :
ApplicationStatLog yes DatePattern yyyy-MM-dd
--
```

2.2.57 TransportStatLog

```
=====
Supported OS : Linux / Windows / Mac
Format : TransportStatLog <flag-available>[ <log-rotation-conf>]
-----
flag-available
Default : no
Range of Values : yes, no
-----
log-rotation-conf
Format : ( FileSize <file-size> <backups> | DatePattern <date-pattern> )
-----
file-size
Default : none
Range of Values : signed double-length integer
-----
backups
Default : none
Range of Values : unsigned integer
-----
date-pattern
Default : none
Range of Values : yyyy-MM, yyyy-MM-dd, yyyy-MM-dd-HH, yyyy-MM-dd-HH-mm
=====
```

The configuration on the transport statistics is set.

When “yes” in flag-available, the transport statistics data is output.

log-rotation-conf specifies the rotation rule. It works in the same way as the rotation behavior set in “TransportStatLog” on hcpd.

Based on the paths specified in “FileSize” and “DatePatternas” as each criterion, the rotations are carried out as below.

```
// FileSize cases
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>.1
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>.2
...
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>.n
// DatePattern cases
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>.2019-12-10
<specified path>.transport.tcp.service_<service number>.<service port number>.<thread number>.2019-12-09
...
```

The header of the statistics information is not included in rotated files.

```
--
Example1 :
TransportStatLog yes
Example2 :
TransportStatLog yes FileSize 10MB 10
Example3 :
TransportStatLog yes DatePattern yyyy-MM-dd
--
```

2.2.58 UDPTransportExtensionBufferSize

```
=====
Supported OS : Linux / Windows / Mac
Format : UDPTransportExtensionBufferSize <ext-buf-size>
-----
ext-buf-size
Default : 2GB
Range of Values : unsigned double-length integer (byte)
=====
```

The extended buffer size for HpFP (UDP) transport is set.

In HpFP sessions, the buffer size for transmission can be extended to the size specified in “hpfp_sndbuf” or “hpfp_rcvbuf” of “UDPListenAddress”, adjusting to delays and

packet-losses or an increase of traffic. The total extended buffer is controlled to be up to the specified value.

When “0”, the total buffer size is not controlled.

The default buffer size (before extended) is 1MB.

--

Example :

```
UDPTransportExtensionBufferSize 4GB
```

--

2.2.59 TCPTransportSocketSendBuffer

=====

Supported OS : Linux / Windows / Mac

Format : TCPTransportSocketSendBuffer <snd-buf-size>

snd-buf-size

Format : <decimal_number>[[(T|G|M|K)]B]

Default : 0

Range of Values : unsigned double-length integer (byte)

=====

Specifies a TCP sending buffer size in bytes. 0 indicates no specification of this option.

You need this option to make a performance tuning of TCP on 100G environment. No need to use in ordinary cases.

--

Example :

```
TCPTransportSocketSendBuffer 128MB
```

--

2.2.60 PubkeyAuthenticationPrior

=====

Supported OS : Linux / Windows / Mac

Format : PubkeyAuthenticationPrior <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

Whether public key authentication (public key authentication) takes priority is set.

When “yes”, first, it searches and loads the private key. In the case that it is encrypted, the password to decrypt it is requested (not supported on the Windows versions). The

first successfully loaded RSA key is supposed to be authenticated (the others are ignored). When the private key load is not successful, Password authentication is tried.

When “no”, conventional authentication takes place. In the case of missing password, inputting the password is requested, and all authentication methods are tried.

--

Example :

PubkeyAuthenticationPrior no

--

2.2.61 ApplicationStatLogSecurityEx

=====

Supported OS : Linux / Windows / Mac

Format : ApplicationStatLogSecurityEx <flag-available>

flag-available

Default : yes

Range of Values : yes, no

=====

Whether to output detailed information on the security in the application statistics log is set.

--

Example :

ApplicationStatLogSecurityEx no

--

2.2.62 DiskBenchmarkPreAllocation

=====

Supported OS : Linux

Format : DiskBenchmarkPreAllocation <how-to-pre-alloc>

how-to-pre-alloc

Default : none

Range of Values : none, native, posix

=====

This option specifies how to make pre-allocation of storage in some disk writing benchmarks performed by the run-host-benchmark option.

‘none’ disables the pre-allocation on the benchmarks.

‘native’ indicates making the pre-allocation by the platform dependent function, e.g., fallocate function on Linux.

'posix' indicates making the pre-allocation by the POSIX function as the posix_fallocate function.

This option will be used when performing benchmarks of Async I/O. Writing performance with the pre-allocation might be better than one without.

```
--  
Example :  
DiskBenchmarkPreAllocation native  
--
```

2.2.63 DiskBenchmarkPreAllocationSize

```
=====
Supported OS : Linux
Format : DiskBenchmarkPreAllocationSize <pre-allocation-size>
-----
pre-allocation-size
Default : 0
Range of Values : signed double-length integer
=====
```

This option specifies a unit size in bytes for the pre-allocation of storage described above.

When 0 or negative values are specified, the pre-allocation will be performed in a file size to write each benchmarks (one time allocation).

```
--
Example :
DiskBenchmarkPreAllocationSize 1GB
--
```

2.2.64 DiskBenchmarkDirectAlignmentSize

```
=====
Supported OS : Linux
Format : DiskBenchmarkDirectAlignmentSize <alignment-size>
-----
alignment-size
Default : 0
Range of Values : unsigned double-length integer
=====
```

This option specified an alignment size in memory for writing and reading buffers used for some disk benchmarks with Direct I/O performed by the run-host-benchmark option.

Specification of 0 indicates to detect the size by querying to the system and use its result.

```
--  
Example :  
DiskBenchmarkDirectAlignmentSize 8KB  
--
```

2.2.65 DiskBenchmarkAsyncNoWait (Reserved)

2.2.66 DiskBenchmarkAsyncMaxEvents

```
=====
Supported OS : Linux
Format : DiskBenchmarkAsyncMaxEvents <num-max-events>
-----
num-max-events
Default : 16
Range of Values : signed integer
=====
```

This option specifies a maximum number of events processed at once in some disk benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

For example, when a result of writing performance is under an expected one with striped storages, the result might be improved increasing the maximum number.

```
--
Example :
DiskBenchmarkAsyncMaxEvents 32
--
```

2.2.67 DiskBenchmarkAsyncMaxGetEvents

```
=====
Supported OS : Linux
Format : DiskBenchmarkAsyncMaxGetEvents <num-max-get-events>
-----
num-max-get-events
Default : 1
Range of Values : signed integer
=====
```

This option specified a maximum number of events to take its results at once in the benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

It is used for observing changes of performance characteristics increasing the number of results being taken at once.

--

Example :

DiskBenchmarkAsyncMaxGetEvents 4

--

2.2.68 DiskBenchmarkAsyncRequestPoolSize

=====

Supported OS : Linux

Format : DiskBenchmarkAsyncRequestPoolSize <pool-size>

pool-size

Default : 32

Range of Values : unsigned integer

=====

This option specifies a size of a pool holding user buffers as I/O requests in some disk benchmarks with Asynchronous I/O performed by the run-host-benchmark option.

--

Example :

DiskBenchmarkAsyncRequestPoolSize 64

--

2.2.69 DeepDiskBenchmarkFileSize

=====

Supported OS : Linux

Format : DeepDiskBenchmarkFileSize <file-size>

file-size

Default : 16GB

Range of Values : signed double-length integer

=====

This option specifies a file size used in some additional disk benchmarks performed by the run-host-benchmark option.

--

Example :

DeepDiskBenchmarkFileSize 32GB

--

2.2.70 DeepDiskBenchmarkFreeSpaceRequired

=====

Supported OS : Linux

Format : DeepDiskBenchmarkFreeSpaceRequired <free-space-size>

free-space-size

Bytix Archaea tools Command Reference

Default : 32GB

Range of Values : unsigned double-length integer

=====

This option specifies a disk free space required in some additional disk benchmarks performed by the run-host-benchmark option.

--

Example :

DeepDiskBenchmarkFreeSpaceRequired 64GB

--

2.2.71 DeepDiskBenchmarkBlockSizes

=====

Supported OS : Linux

Format : DeepDiskBenchmarkBlockSizes <block-size-set-desc>

block-size-set-desc

Default : 16KB 32KB 64KB 128KB 256KB 512KB 1MB 2MB

Range of Values : a set of block sizes separated with white spaces

=====

This option specifies a set of block sizes used in some additional disk benchmarks performed by the run-host-benchmark option.

--

Example :

DeepDiskBenchmarkBlockSizes 64KB 256KB 512KB 1MB

--

2.3 hcp.conf

name	description
Include	include external configuration file
UseProperCopyAndSync	cp/synchronizationn setting
AtomicLikeSaving	atomically file saving
AtomicLikeSavingThreshold	threshold for atomically file saving
AutoResumeTrials	nummber of auto resume trials
AutoResumeTrialInterval	auto resume interval in seconds
MemoryTransferConcurrency	memory copy concurrency
MaxReadRate	Disk I/O reading rate per session
MaxWriteRate	Disk I/O writing rate per session

2.3.1 Include

```
=====
Supported OS : Linux / Windows / Mac
Format : Include <file-path>
-----
file-path
Default : none
Range of Values : path string of file system
=====
```

The file written the common configurations among client commands is done “Include”. “Include” can be written anywhere in the hcp.conf. The value of Include is overwritten. “Include” can’t be nested.

```
--
Example :
Include /etc/hcp/hcp-common.conf
--
```

When you specifies file-path in a relative path, the software tries to find it as a file path relative from the file where you describe the Include statement.

2.3.2 UseProperCopyAndSync

```
=====
Supported OS : Linux / Windows / Mac
Format : UseProperCopyAndSync <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When it comes to copy or synchronization, it is controlled to follows the cp or rsync command policy.

Copy behaviors are mainly changed into the following.

- When a source directory is specified and the destination path exists as specified, the same name directory as the source is created in the destination, and the files are copied under the directory.
- When a source directory is specified and the destination path doesn’t exist as specified, the same name directory as the destination path is created in the destination, and the files are copied under the directory (the same name directory as the source is not created).
- In overwriting, in the case that the file types are not coincident between source and destination (ex: a file name in the source is a directory name in the

destination,) it shows an error message with the reason code (CANNOT_OVERWRITE_DIR or CANNOT_OVERWRITE_NON_DIR)

- When a directory is specified in the source without the -R option (recursive copy), it shows an error message with the reason code, OMIT_DIR.
- When plural paths are specified in the source and the destination path is not a directory, it stops executing the command with the reason code, DEST_IS_NON_DIR.
- When the source may include plural files (a directory, or Wild card, or with regular expression options,) and also the destination path exists but is not a directory, it stops executing the command with the reason code CANNOT_OVERWRITE_NON_DIR.

When synchronizing, the followings are the major behavior changes.

- When a directory is specified in the source, and the path doesn't have a trailing slash (/), the same name directory as one in the source is created in the destination path directory (if not exist, newly created), where the file is copied.
- When a destination directory is specified, and the path also has a trailing slash (/), the file is copied in the destination path's directory.(if not exist, newly created).
- When the file types are not coincident between source and destination in overwriting (ex: a file name in the source is a directory name in the destination), it is overwritten after deleting the file or directory in the destination.
- When a directory is specified in the source without the -R option (recursive copy), the command is skipped with the reason code, OMIT_DIR.However, the command result is not recorded as an error (the exit status 0).
- When the source may include plural files (a directory, or Wild card, or with regular expression options,) and also the destination path exists but is not a directory, it stops executing the command with the reason code CANNOT_OVERWRITE_NON_DIR.

--

Example :

UseProperCopyAndSync no

--

2.3.3 AtomicLikeSaving

Refer to the hcpd configurations.

2.3.4 AtomicLikeSavingThreshold

Refer to the hcpd configurations.

2.3.5 AutoResumeTrials

```
=====
Supported OS : Linux / Windows / Mac
Format : AutoResumeTrials <num-trials>
-----
num-trials
Default : -1
Range of Values : signed integer
=====
```

This option specifies a number of trials of auto resumes. -1 indicates unlimited number of trials. When 0 is set, hcp will stop without resuming.

```
--
Example :
AutoResumeTrials 5
--
```

2.3.6 AutoResumeTrialInterval

```
=====
Supported OS : Linux / Windows / Mac
Format : AutoResumeTrialInterval <trial-interval>
-----
trial-interval
Default : 30
Range of Values : unsigned integer
=====
```

This option specifies an interval of waiting for the next auto resume in seconds.

```
--
Example :
AutoResumeTrialInterval 10
--
```

2.3.7 MemoryTransferConcurrency

```
=====
Supported OS : Linux / Windows / Mac
Format : MemoryTransferConcurrency <num-concur> <wait-type> <busy-sleep-n
sec>
-----
num-concur
Default : auto (smaller value of physical-CPUs/2 or 16)
Range of Values : unsigned integer
-----
wait-type
Default : cond
```

Range of Values : cond, busy

busy-sleep-nsec

Default : 1

Range of Values : unsigned integer

=====

When you use -n option on the hcp command which starts the command on memory-to-memory transfer mode, this option configures how to copy memory data of file payloads in concurrent way at the sender side.

num-concur specifies a number of concurrent copies. 1 indicates the standar memory copy by memcpy without concurrency.

wait-type specifies a waiting method on memory copy threads in its idling state. cond is to perform a conditinal wait on that idling state and busy is to perform a busy wait on it. When busy is set, CPU usage might be up to a multiplication of the number of CPUs and 100%.

busy-sleep-nsec specifies a waiting time in nano seconds on the busy wait.

This options is defined for a performance tuning to remove performance limitation by a single threaded memory copy on 100Gbps network environment.

--

Example :

MemoryTransferConcurrency 1 cond 1 # To disable

MemoryTransferConcurrency 12 busy 1 # Busy wait, 4 concurrent and wait in
1 nano seconds

--

2.3.8 MaxReadRate

=====

Supported OS : Linux / Windows / Mac

Format : MaxReadRate <read-rate>

read-rate

Default : 10Ebit (Unlimited)

Range of Values : unsigned double-length integer (up to 10Ebit)

=====

This option specifies limitation of reading data from files on file transfer. This will be applied to each session which performs the file transfer. It is recognized as unlimited when the value is the maximum value in bps or over it.

In some environment, long time running of reading and writing might make overheat on SSDs (especially the writing side). So this option is useful for avoiding it.

--

Example :

MaxReadRate 10Gbit

--

2.3.9 MaxWriteRate

```
=====
Supported OS : Linux / Windows / Mac
Format : MaxWriteRate <write-rate>
-----
write-rate
Default : 10Ebit (Unlimited)
Range of Values : unsigned double-length integer (up to 10Ebit)
=====
```

This option specifies limitation of writing data to files on file transfer. This will be applied to each session which performs the file transfer. It is recognized as unlimited when the value is the maximum value in bps or over it.

In some environment, long time running of reading and writing might make overheat on SSDs (especially the writing side). So this option is useful for avoiding it.

--

Example :

MaxWriteRate 10Gbit

--

2.4 hsync.conf

name	description
Include	include external configuration files
AutoRerunTrials	nummber of auto rerun trials
AutoRerunTrialInterval	auto rerun interval in seconds

2.4.1 Include

Refer to hcp.conf

2.4.2 AutoRerunTrials

```
=====
Supported OS : Linux / Windows / Mac
Format : AutoRerunTrials <num-trials>
-----
num-trials
Default : -1
Range of Values : signed integer
=====
```

This option specifies a number of trials of auto reruns. -1 indicates unlimited number of trials. When 0 is set, hcp will stop without rerunning.

```
--  
Example :  
AutoRerunTrials 5  
--
```

2.4.3 AutoRerunTrialInterval

```
=====
Supported OS : Linux / Windows / Mac
Format : AutoRerunTrialInterval <trial-interval>
-----
trial-interval
Default : 30
Range of Values : unsigned integer
=====
```

This option specifies an interval of waiting for the next auto rerun in seconds.

```
--
Example :
AutoRerunTrialInterval 10
--
```

2.5 hrm.conf

name	description
Include	include external configuration files

2.5.1 Include

Refer to hcp.conf

2.6 hcp-ls.conf

name	description
Include	include external configuration files

2.6.1 Include

Refer to hcp.conf

2.7 hmkdir.conf

name	description
Include	include external configuration files

2.7.1 Include

Refer to hcp.conf

2.8 hpwd.conf

name	description
Include	include external configuration files

2.8.1 Include

Refer to hcp.conf

2.9 hmv.conf

name	description
Include	include external configuration files

2.9.1 Include

Refer to hcp.conf

2.10 hln.conf

name	description
Include	include external configuration files

2.10.1 Include

Refer to hcp.conf

2.11 hchmod.conf

name	description
Include	include external configuration files

2.11.1 Include

Refer to hcp.conf

2.12 hchown.conf

name	description
Include	include external configuration files

2.12.1 Include

Refer to hcp.conf

2.13 users

The users that the hcpd daemon can authenticate or it modifies how to authenticate are defined in the following format below.

Format : [!]<username>:<auth_methods>:[<mapping_uid>]:[<mapping_gid>[,<mapping_sgid>...]]:[<hpfp_cong_modes>][:umask <umask_val>[<dir_umask_val>]]:[<home_dir>]

In the username, the user name is described. Characters except for separators are available. Even a string that does not exist as any system user (a user name specific for Bytix Archaea tools) can be specified. Entries starting with an exclamation mark '!' tells hcpd to reject authentication of users corresponding to the entries.

In the auth_methods, the user available authentication methods can be described successionaly by delimiting with commas (,) as follows.

- LPA
- PAM
- PKA (RSA)
- WLU

UID for the user is described in mapping_uid. When not described, it is inquired to the system using the user name.

GID as the primary group for the user is described in mapping_gid. And GIDs of supplemental groups are described in mapping_sgid by delimiting with commas (,).

One of the 3 user available congestion control modes, such as MODEST, FAIR_FAST_START, or AGGRESSIVE (or each abbreviation, M, F, or A) on HpFP transport is set as hpfp_cong_modes. If the mode isn't set, default is FAIR mode.

umask_val specifies a umask value that you want to apply to the user. When this option is set, the value of PrivilegeSeparationUmask will not be applied to the user. If you set different values for files and directories respectively, please use dir_umask_val specifying a value to be applied to directories. When any value of this option is not set like "...:umask:...", hcpd consider the option is not set and apply a value of PrivilegeSeparationUmask to the user. Please see the description of PrivilegeSeparationUmask for how the umask_val and dir_umask_val work.

home_dir shows this home directory. If not described, hcpd queries the system about it by the user name.

--

Example :

hcp_user:LPA,PKA:1000:1000::/home/user

```
user:PAM:::  
user:PAM:::umask 0007:  
user01:PAM::1000,967,10::  
--
```

2.14 passwd

The user credentials (the hashed password) that the hcpd daemon uses in LPA credentials is defined in the following format.

Format : <username>:<hash_method>:<hash_value>

The user name is set in username.

hash_method is set as the way to create the authentication information from the below options.

- md5
- sha
- sha224
- sha256
- sha384
- sha512

The hashed string which was transformed following the formula below is set in hash_value.

hex_string (hash_function (<user input password>))

hex_string is a function to transform binary data to hexadecimal string.

hash_function is the digest function set in hash_method.

This string can be generally created by using the operating system tool as below.

```
$ echo -n my_password | openssl dgst -md5  
(stdin)= a865a7e...93bea4
```

--

Example :

```
# password is "password01"
```

```
hcp_user:sha256:4b8f353889d9a05d17946e26d014efe99407cba8bd9d0102d4aab10ce  
6229043
```

--

3 Statistics reference

3.1 Application statistics

After operations such as file transfers (hcp) and file deletions (hrm) and so on applications, those output information is recorded in the specific files on the client and server.

column name	descripn
Start Date_Time	start date and time
End Date_Time	end date and time
Exit	exit code
Remote Host	remote host
User	user name
Application	application name
Total	total transmission data (byte)
Payload	file data transmission (byte)
Files	the number of files
Directories	the number of directories
Average Throughput	average throughput (bps)
Encoding	transport string encoding
Security	transport security
Compression	compression
Proto	transport protocol
Local	local address and port number
Foreign	remote address and port number
PID	process ID

The application operation start date and time is recorded in the following format in Start Date_Time.

yyyy/mm/dd HH:MM::SS

The application operation end date and time is recorded in the following format in End Date_Time.

yyyy/mm/dd HH:MM::SS

Bytix Archaea tools Command Reference

The file process reason code (described later) is recorded as the application operation end code in Exit with the following format.

The host name or IP address of the remote host is recorded in Remote Host.

The user who operated the application and the way how to operate it, are recorded in User. When it is not authenticated, anonymous is output.

The application name that created this record is recorded in Application, which is supposed to be one of those below.

- hcp (tx|rx)
- hsync (tx|rx)
- hrm
- hcp-ls
- hmkdir
- hpwd
- hmv
- hln
- hchmod
- hchown

The protocol version in which the application was operated is described as below (in the order of protocol number, protocol revision number).

..., hcp (tx) [3.1], ...

The total transmission data on the application layer (including the data to control file requests) is recorded in Total.

The total payload on the application layer (the total size of file data in file transfers) is recorded in Payload.

The number of the files which was processed on the application layer is recorded in Files (which doesn't include directories).

The number of the directories which was processed on the application layer is recorded in Directories.

The average throughput on the application layer is recorded in Average Throughput.

The processed transport string encodings are recorded in Encoding.

The processed transport security is recorded in Security. The purpose of usage of the digest algorithm is added as the following names.

- MAC (the identification test of message data in session encryption)

- Chunk (the test of data chunks of files)
- File (the file test)

In encrypted sessions, when the data integrity checking is disabled, “MAC” is not added.

- RequireDataIntegrityChecking (hcpd.conf)
- DisableDataIntegrityChecking (hcp.conf)

When ApplicationStatLogSecurityEx is yes, the following information on the transport security is added to the log.

- Bxxx (cryptographic algorithm block size. xxx is the block size (bit.))
- Kxxx (cryptographic algorithm key size. xxx is the key size (bit.))
- HmacXxx/VmacXxx (Data integrity check modeXxx is the algorithm name.)

The processed compression mode (the compression level, header compression or content compression on/off) is recorded in Compression.

The processed transport protocol is recorded in Proto. In this version, one of the following is output.

- TCP
- HpFP
- WSS
- WS

When HpFP is recorded, the chosen congestion control mode is added as the following names.

- F (Fair mode)
- S (Fair Fast mode)
- A (Aggressive mode)
- M (Modest mode)
- N (none)

And a maximum value of detected MSS is also recorded.

When a session has multiple connections, the number of connections is noted in parenthesis beside the transport protocol.

The IP address or port number of the local end of the transport session (end point) is recorded in Local.

The IP address or port number of the remote end of the transport session (end point) is recorded in Foreign.

Bytix Archaea tools Command Reference

The application process ID is recorded in PID.

--

Example :

Client

```
Start Date_Time, End Date_Time, Exit, Remote Host, User, Application, Total (bytes), Payload (bytes), Files, Directories, Average Throughput (bps), Encoding, Security, Compression, Proto, Local, Foreign, PID
2025/01/06 16:27:24, 2025/01/06 16:27:30, 0000, 127.0.0.1, user, hcp (tx) [3.1], 8590723508, 8589934592, 1, 0, 10703091712.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC / B128 K256 VmacAES64], None, TCP, 127.0.0.1:40920, 127.0.0.1:874, 74612
2025/02/02 14:55:36, 2025/02/02 14:55:36, 0000, 192.168.30.52, user, hcp (tx) [3.1], 1053400, 1048641, 1, 0, 21563498.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA256], None, TCP, 192.168.30.51:35858, 192.168.30.52:874, 3651
2025/02/02 15:28:24, 2025/02/02 15:28:24, 0000, 192.168.30.52, user, hcp (tx) [3.1], 1052440, 1048641, 1, 0, 21731128.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [B128 K256], None, TCP, 192.168.30.51:35890, 192.168.30.52:874, 3832
2025/02/02 15:10:50, 2025/02/02 15:10:50, 0000, 192.168.30.52, user, hcp (tx) [3.1], 1053400, 1048641, 1, 0, 21753950.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K128 HmacSHA256], None, TCP, 192.168.30.51:35864, 192.168.30.52:874, 3727
2025/02/02 15:19:57, 2025/02/02 15:19:58, 0000, 192.168.30.52, user, hcp (tx) [3.1], 1050772, 1048641, 1, 0, 19767822.000000, UTF8, None SHA256, None, TCP, 192.168.30.51:35880, 192.168.30.52:874, 3794
2025/02/02 15:29:37, 2025/02/02 15:19:58, 0000, 192.168.30.52, user, hcp (tx) [3.1], 1050772, 1048641, 1, 0, 19767822.000000, UTF8, None SHA256, None, TCP (8), 192.168.30.51:35880, 192.168.30.52:874, 3794
2025/02/02 17:31:25, 2025/02/02 17:31:25, 0000, 127.0.0.1, user, hcp (rx) [3.1], 2160, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC], None, HpFP [N / MSS1456], 127.0.0.1:54918, 127.0.0.1:884, 41340
2025/02/02 17:32:28, 2025/02/02 17:32:28, 0000, 127.0.0.1, user, hcp (rx) [3.1], 2160, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC / B128 K256 VmacAES], None, HpFP [N / MSS1456], 127.0.0.1:21373, 127.0.0.1:884, 41458
2025/02/02 17:33:41, 2025/02/02 17:33:41, 0000, 127.0.0.1, user, hcp (rx) [3.1], 2480, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA256], None, HpFP [N / MSS1456], 127.0.0.1:50812, 127.0.0.1:884, 41556
2025/02/02 17:43:21, 2025/02/02 17:33:41, 0000, 127.0.0.1, user, hcp (rx) [3.1], 2480, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA256], None, HpFP [N / MSS1456] (8), 127.0.0.1:50812, 127.0.0.1:884, 41556
```

Server

```

Start Date_Time, End Date_Time, Exit, Remote Host, User, Application, Total (bytes), Payload (bytes), Files, Directories, Average Throughput (bps), Encoding, Security, Compression, Proto, Local, Foreign, PID
2025/01/08 14:35:45, 2025/01/08 14:35:45, 0000, 127.0.0.1:37100, user [PK A], hcp (tx) [3.1], 3428, 1024, 1, 0, 20145.384766, UTF8, AES/CTR/NoPadding SHA256 [B128 K256], None, TCP, 127.0.0.1:874, 127.0.0.1:37100, 57562
2025/01/08 14:36:10, 2025/01/08 14:36:10, 0000, 127.0.0.1:37102, user [PK A], hcp (tx) [3.1], 3428, 1024, 1, 0, 19958.435547, UTF8, AES/CTR/NoPadding SHA256, None, TCP, 127.0.0.1:874, 127.0.0.1:37102, 57650
2025/01/08 15:26:30, 2025/01/08 14:36:10, 0000, 127.0.0.1:37102, user [PK A], hcp (tx) [3.1], 3428, 1024, 1, 0, 19958.435547, UTF8, AES/CTR/NoPadding SHA256, None, TCP (8), 127.0.0.1:874, 127.0.0.1:37102, 57650
2025/02/02 17:31:25, 2025/02/02 17:31:25, 0000, 127.0.0.1:54918, user [PA M], hcp (tx) [3.1], 2160, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC], None, HpFP [N / MSS1456], 127.0.0.1:884, 127.0.0.1:54918, 41349
2025/02/02 17:32:28, 2025/02/02 17:32:28, 0000, 127.0.0.1:21373, user [PA M], hcp (rx) [3.1], 2160, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC / B128 K256 VmacAES], None, HpFP [N / MSS1456], 127.0.0.1:884, 127.0.0.1:21373, 41465
2025/02/02 17:33:41, 2025/02/02 17:33:41, 0000, 127.0.0.1:50812, user [PA M], hcp (rx) [3.1], 2480, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA256], None, HpFP [N / MSS1456], 127.0.0.1:884, 127.0.0.1:50812, 41563
2025/02/02 17:43:21, 2025/02/02 17:33:41, 0000, 127.0.0.1:50812, user [PA M], hcp (rx) [3.1], 2480, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA256], None, HpFP [N / MSS1456] (8), 127.0.0.1:884, 127.0.0.1:50812, 41563
--

```

3.2 Transport statistics

3.2.1 TCP statistics

During TCP communications, the amount of communication and the transport statistics are recorded periodically (every 1 sec).

column name	description
Date_Time	recorded date and time
Tx	transmitting data size (byte)
Rx	receiving data size (byte)
AcqTx	acquired transmitting bandwidth (byte)
AcqRx	acquired receiving bandwidth (byte)
Cwnd	congestion window size (byte)
RTT	RTT (microsecond)

Bytix Archaea tools Command Reference

Retrans	the number of retransmission
TpTx	transmitting throughput (bps)
TpRx	receiving throughput (bps)
AvgTpTx	average transmitting throughput (bps)
AvgTpRx	average receiving throughput (bps)

The date and time when this record was created is recorded in Date_Time in the following format.

yyyy/mm/dd HH:MM::SS.uuuuuu (described by microsecond)

The number of data (byte) which has been transmitted on the transport layer before this record was created is recorded in Tx (difference).

The number of data (byte) which has been received on the transport layer before this record was created is recorded in Rx (difference).

The transmitting bandwidth (byte) acquired on the transport layer until this record was created is recorded in AcqTx (difference).

The receiving bandwidth (byte) acquired on the transport layer until this record was created is recorded in AcqRx (difference).

The congestion window size acquired from TCP statistics information at the time when this record is created is recorded in Cwnd.

RTT acquired from TCP statistics information at the time when this record is created is recorded in RTT.

The retransmission count acquired from TCP statistics information at the time when this record is created is recorded in Retrans.

The transmitting throughput on the transport layer is recorded in TpTx.

The receiving throughput on the transport layer is recorded in TpRx.

The average transmitting throughput on the transport layer is recorded in AvgTpTx.

The average receiving throughput on the transport layer at the time when this record is created is recorded in AvgTpRx.

--

Example :

--

PID 11168, Local 127.0.0.1:58374, Foreign 127.0.0.1:11111
Date_Time, Tx (bytes), Rx (bytes), AcqTx (bytes), AcqRx (bytes), Cwnd (bytes), RTT (usec), Retrans, TpTx (bps), TpRx (bps), AvgTpTx (bps), AvgTpRx

```
(bps)
2018/05/25 15:05:50.142156, 0, 0, 0, 0, 218450, 17, 0, 0.000000, 0.000000,
0.000000, 0.000000
2018/05/25 15:05:52.868790, 2288, 1760, 2288, 1764, 654830, 21, 0, 6712.9
42871, 5163.802246, 6712.854004, 5163.731934
2018/05/25 15:05:53.321617, 4436, 2920, 4436, 2920, 654830, 12764, 0, 783
69.882812, 51587.031250, 16918.314453, 11775.388672
--
```

3.2.2 HpFP statistics

During HpFP communicating, The traffic and transport statistics are recorded periodically (approximately every 1 second) on the server and client.

column	description
Date_Time	recorded date and time
Tx	transmitting data size (byte)
Rx	receiving data size (byte)
AcqTx	acquired transmitting bandwidth (byte)
AcqRx	acquired receiving bandwidth (byte)
Cwnd	congestion window size (byte)
RTT	RTT (microsecond)
Retrans	the bytes of retransmission
Congestion	congestion detection count
MSS	MSS (byte)
MaxTp	maxmum throughput (bps)
LongCtxWait	long time count to wait for the context
TpTx	transmitting throughput (bps)
TpRx	receiving throughput (bps)
AvgTpTx	average transmitting throughput (bps)
AvgTpRx	average receiving throughput (bps)

The date and time when this record was created is recorded in Date_Time in the following format.

yyyy/mm/dd HH:MM::SS.uuuuuu (described by microsecond)

The number of data (byte) which has been transmitted on the transport layer before this record is created is recorded in Tx (difference).

The number of data (byte) which has been received on the transport layer before this record is created is recorded in Rx (difference).

The transmitting bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqTx (difference).

The receiving bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqRx (difference).

The congestion window size acquired from HpFP statistics information at the time when this record is created is recorded in Cwnd.

RTT acquired from TCP statistics information at the time when this record is created is recorded in RTT.

The retransmission count acquired from TCP statistics information at the time when this record is created is recorded in Retrans.

The congestion detection count (cumulative value) acquired from HpFP statistics information at the time when this record is created is recorded in Congestion.

MSS acquired from HpFP statistics information at the time when this record is created is recorded in MSS.

The maximum throughput from the HpFP statistics information at the moment when this record is created is recorded in MaxTp.

The long time waiting count for the context from the HpFP statistics information at the moment when this record is created is recorded in LongCtxWait. When it is counting up, it may be causing the influence on the performance by the context switch.

The transmitting throughput on the transport layer is recorded in TpTx.

The receiving throughput on the transport layer is recorded in TpRx.

The average transmitting throughput on the transport layer is recorded in AvgTpTx.

The average receiving throughput on the transport layer at the time when this record is created is recorded in AvgTpRx.

--

Example :

--

```
PID 2848, Local 127.0.0.1:63304, Foreign 127.0.0.1:884
Date_Time, Tx (bytes), Rx (bytes), TxAcq (bytes), RxAcq (bytes), Cwnd (bytes),
RTT (usec), Retrans (bytes), Congestion, MSS (bytes), MaxTp (bps),
LongCtxWait, TpTx (bps), TpRx (bps), AvgTpTx (bps), AvgTpRx (bps)
2019/10/30 09:34:17.520056, 0, 0, 0, 0, 89560, 382, 0, 0, 1236, 0, 0, 0.0
```

```
00000, 0.000000, 0.000000, 0.000000
2019/10/30 09:34:19.915566, 1052, 1124, 1052, 66536, 89560, 382, 0, 0, 12
36, 5536, 0, 3511.808594, 3752.160400, 3511.798340, 3752.149414
2019/10/30 09:34:20.300687, 1708, 620, 1708, 744, 89560, 43, 0, 0, 1236,
85832, 0, 35479.757812, 12879.069336, 7937.694824, 5015.702637
--
```

3.2.3 WS/WSS statistics

During WS/WSS communicating, The traffic and transport statistics are recorded periodically (approximately every 1 second) on the server and client.

column	description
Date_Time	recorded date and time
Tx	transmitting data size (byte)
Rx	receiving data size (byte)
AcqTx	acquired transmitting bandwidth (byte)
AcqRx	acquired receiving bandwidth (byte)
Cwnd	congestion window size (byte)
RTT	RTT (microsecond)
Retrans	the number of retransmission
TpTx	transmitting throughput (bps)
TpRx	receiving throughput (bps)
AvgTpTx	average transmitting throughput (bps)
AvgTpRx	average receiving throughput (bps)

The date and time when this record was created is recorded in Date_Time in the following format.

yyyy/mm/dd HH:MM::SS.uuuuuu (described by microsecond)

The number of data (byte) which has been transmitted on the transport layer before this record is created is recorded in Tx (difference).

The number of data (byte) which has been received on the transport layer before this record is created is recorded in Rx (difference).

The transmitting bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqTx (difference).

The receiving bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqRx (difference).

The congestion window size acquired from TCP statistics information at the time when this record is created is recorded in Cwnd.

RTT acquired from TCP statistics information at the time when this record is created is recorded in RTT.

The retransmission count acquired from TCP statistics information at the time when this record is created is recorded in Retrans.

The transmitting throughput on the transport layer is recorded in TpTx.

The receiving throughput on the transport layer is recorded in TpRx.

The average transmitting throughput on the transport layer is recorded in AvgTpTx.

The average receiving throughput on the transport layer at the time when this record is created is recorded in AvgTpRx.

--

Example :

--

```
PID 11168, Local 127.0.0.1:58374, Foreign 127.0.0.1:11111
Date_Time, Tx (bytes), Rx (bytes), AcqTx (bytes), AcqRx (bytes), Cwnd (bytes),
RTT (usec), Retrans, TpTx (bps), TpRx (bps), AvgTpTx (bps), AvgTpRx (bps)
2018/05/25 15:05:50.142156, 0, 0, 0, 0, 218450, 17, 0, 0.000000, 0.000000,
0.000000, 0.000000
2018/05/25 15:05:52.868790, 2288, 1760, 2288, 1764, 654830, 21, 0, 6712.9
42871, 5163.802246, 6712.854004, 5163.731934
2018/05/25 15:05:53.321617, 4436, 2920, 4436, 2920, 654830, 12764, 0, 783
69.882812, 51587.031250, 16918.314453, 11775.388672
--
```

3.3 System statistics

During the server (the hcpd daemon) processing, The traffic and the access statistics and status are recorded periodically (approximately every 10 second).

column	description
Date_Time	recooded date and time
Tx	transmitting data size (byte)
Rx	receiving data size (byte)
AcqTx	acquired transmitting bandwidth (byte)
AcqRx	acquired receiving bandwidth (byte)
Conn	the number of incoming connections

TCPConn	the number of incoming TCP connections
HpFPConn	the number of incoming HpFP connections
UserConn	the number of incoming users
WorkConn	the number of processing connections
WorkTCPConn	the number of processing TCP connections
WorkHpFPConn	the number of processing HpFP connections

The date and time when this record was created is recorded in Date_Time in the following format.

yyyy/mm/dd HH:MM::SS.uuuuuu (described by microsecond)

The number of data (byte) which has been transmitted on the transport layer before this record is created is recorded in Tx (difference).

The number of data (byte) which has been received on the transport layer before this record is created is recorded in Rx (difference).

The transmitting bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqTx (difference).

The receiving bandwidth (byte) which has been acquired on the transport layer before this record is created is recorded in AcqRx (difference).

The number of incoming connections which has been connected before this record is logged is recorded in Conn (difference).

The number of incoming TCP connections which has been connected before this record is logged is recorded in TCPConn (difference).

The number of incoming HpFP connections which has been connected before this record is logged is recorded in HpFPConn (difference).

The number of incoming users which has been connected before this record is logged is recorded in UserConn (difference).

The number of processing communications at the time is recorded in WorkConn (present value).

The number of processing TCP communications at the time is recorded in WorkTCPConn (present value).

The number of processing HpFP communications at the time is recorded in WorkHpFPConn (present value).

--

Example :

--

```
Date_Time, Tx (bytes), Rx (bytes), AcqTx (bytes), AcqRx (bytes), Conn, TC
PConn, HpFPConn, UserConn, WorkConn, WorkTCPConn, WorkHpFPConn
2018/07/05 18:17:40.657653, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
2018/07/05 18:17:50.666458, 4624, 5688, 4624, 5696, 2, 1, 1, 1, 1, 0, 1
2018/07/05 18:17:52.910125, 2624, 4120, 2624, 4124, 0, 0, 0, 1, 0, 0, 0
```

--

4 Error code reference

4.1 Command end status

These end codes shown below, the data range from 0 to 255, are sent as the result of the execution after each command execution.

exit code	name	description
0	EXIT_SUCCESS	successful
1	EXIT_FAILURE	failure (general)
21	EXIT_NOTICE	exit with notice
40	EXIT_PENDING	pending (reserved)
50	EXIT_WARN	warning (reserved)
71	EXIT_ERROR_CONNECT_FAILED	connection failure
72	EXIT_ERROR_AUTH_FAILED	authentication failure
73	EXIT_ERROR_CONNECTION_FAILURE	connection failure
79	EXIT_ERROR_NEG_FAILED	negotiation failure
81	EXIT_ERROR_IO_FAILURE	application I/O failure (because of the problems of disk or file access)
90	EXIT_ERROR_APP_FAILURE	application processing failure
91	EXIT_ERROR_APP_SETUP_FAILED	application startup failure
99	EXIT_ERROR_APP_ABORTED	application aborted
181	EXIT_ERROR_LOAD_ARG	command argument error
182	EXIT_ERROR_LOAD_CONF	command configuration error
189	EXIT_ERROR_CLI_SETUP_FAILED	CLI startup error
191	EXIT_ERROR_SERVICE_SETUP_FAILED	service startup error

200	EXIT_FATAL	fatal error (general)
201	EXIT_FATAL_RUNTIME_SETUP_FAILURE	fatal environment startup error
202	EXIT_FATAL_MUTEX_SETUP_FAILURE	fatal program synchronization error

4.2 Configuration file error codes

When command errors were found in the configuration file, the exit status of EXIT_ERROR_LOAD_CONF is shown as the result where messages on the detected errors and error code (described below) which shows the kind of reasons are shown on the user interface display.(when on shell applications, standard errors are output) The error codes are shown by the data range (8bit) from 1 to 255.

This error is shown in the following format.

Format : <config_path>: [<error_code>] <message>

“config_path” shows the path of the configuration file where a error occurred.

“error_code” shows the kind of error code why a error occurred.

“message” shows the error message.

--

Example :

```
/etc/hcp/hcp.conf: [052] Configuration file parse error in line 3 : PPubk
eyAuthentication yes
```

--

error code	name	description
0	CONF_ERROR_OK	succeeded (usually it is not displayed)
50	CONF_ERROR_NULL_NAME	acquiring the configuration name failed
51	CONF_ERROR_EMPTY_NAME	the configuration name is vacant
52	CONF_ERROR_UNKNOWN_NAME	it's an unknown configuration name
53	CONF_ERROR_INVALID_NAME	the configuration name is invalid
54	CONF_ERROR_INVALID_VALUE	the value of the configuration name is

		invalid
60	CONF_ERROR_QUOTE_NOT_CLOSED	the quote in the configuration hasn't closed
61	CONF_ERROR_QUOTE_IN_QUOTE	the second quote was found in the quote in the configuration
70	CONF_ERROR_NO_VALUES	there wasn't the onfiguration value
71	CONF_ERROR_TOO_MANY_VALUES	the number of the parameters in the configuration is over the limit
79	CONF_ERROR_OVER_LIMIT_NUM_OF_VALUES	the configuration value is over the maximum
80	CONF_ERROR_UNEXPECTED_NESTED_STRUCT	a nested structured setting was found
81	CONF_ERROR_UNEXPECTED_ENDING_STRUCT	an unexpected structured setting end was found
82	CONF_ERROR_UNEXPECTED_VALUE_OF_STRUCT	an unexpected structured setting item was found
84	CONF_ERROR_ENDING_STRUCT_NOT_FOUND	a structured setting end was not found
85	CONF_ERROR_OVER_LIMIT_NUM_OF_STRUCTS	the number of the parameters in a structured setting is over the limit
99	CONF_ERROR_LINE_LEN_EXCEEDED	the number of the characters in a line exceeded the limit
200	CONF_ERROR_CONF_NOT_FOUND	the configuration file was not found
201	CONF_ERROR_FILE_OPEN_FAILED	opening the configuration file failed
255	CONF_ERROR_FAILURE	failure

4.3 File processing code

Processing results such as file transfer may be output with Reason code listed in the table below as the standard output or a file, e.g. .hcp.out. Reason code ranges from 0 to 65536 and shown in Hexadecimal (16 bit).

Reason code (Hexadecimal)	name	description
0000	NO_ERROR	succeeded
0001	ALREADY_DONE	it was already executed
2C01	NOT_MODIFIED	the file was not updated
2C02	NOT_DIFFERENT	no file difference
2C03	NOT_PERMITTED	the processing was not permitted
2C04	NOT_CONFIRMED_OVERWRITE	overwriting was not permitted
2C05	NOT_CREATED	it was not created
2C06	MODIFIED	already modified
2C07	DIFFERENT	files are different
2C08	MODIFIED_SIZE_IDENT	identical in modified date and time and size
2C09	NOT_EXISTING	dose not exist
2C0A	EXISTING	files existing
2C0B	NOT_MATCH_COND	dose not meet conditions to process
2C0C	DELETED	it was deleted
2C0D	NOT_DELETED	it was not deleted
2C0E	NO_CONTENT_OPERATED	content of files was not processed
2C0F	EXCLUSION_MATCH	meet conditions to exclude processing
2C10	NON_REG_FILE	non-regular file
2FFD	DELETE_EXCLUDED	files to exclude were deleted
2FFE	APP_MAX_EXCEEDED	exceeded limit by application

2FFF	APP_SKIP	skipped by application running condition
9001	UNKNOWN_ENCODING	it is an unknown encoding method
9002	UNKNOWN_BCIPH	it is an unknown cipher method
9003	UNKNOWN_COMPR	it is an unknown compression method
9004	AUTH_REQUIRED	authentication is necessary
9005	FILE_ENTRY_NOT_FOUND	file entry was not found
9006	FILE_ENTRY_ERROR	file entry error
9007	FIND_FILE_ERROR	file search error
9008	AUTH_FAILED	authentication failure
9009	NEG_FAILED	negotiation failure
900A	KEY_EXHG_REQUIRED	security key exchange is necessary
900B	APP_NOT_SUPPORTED	applications (commands) are not supported
9FFB	SESS_IDLE_TIMEOUT	session idle timeout
9FFC	UNEXP_TERM	unexpected termination
9FFD	APP_ABORT	abortion by an application
9FFE	SESS_ABORT	abortion by a session
9FFF	FILE_REQQ_FULL	file queue shortage
A001	FILE_NOT_FOUND	the file was not found
A002	FILE_ALREADY_EXISTS	the file already exists
A003	FILE_ACCESS_DENIED	the file access was denied
A004	DIGEST_ERROR	data integrity check error
A005	WRITE_ERROR	writing file error
A006	CREATE_DIR_ERROR	creating directory failed

Bytix Archaea tools Command Reference

A007	CREATE_LINK_ERROR	creating link failed
A008	READ_ERROR	reading file error
A009	IS_DIR	the directory was detected
A00A	IS_NOT_DIR	the directory wasn't detected
A00B	RENAME_ERROR	file rename error
A00C	DELETE_ERROR	file deletion error
A00D	FILE_IDENT	file identification error
A00E	OP_NOT_PERMITTED	operation is not permitted
A00F	MODIFY_ERROR	file attribute modification error
A010	CANNOT_OVERWRITE_DIR	cannot overwrite directories
A011	CANNOT_OVERWRITE_NON_DIR	cannot overwrite non-directory
A012	DEST_IS_NOT_DIR	the destination is not a directory
A013	OMIT_DIR	directory omitted
A014	TMP_FILE_SETUP_ERROR	temporary file making error
A015	TMP_FILE_FIX_ERROR	temporary file fixing error
A016	CREATE_DEVICE_ERROR	device creation error
A017	CREATE_SPECIAL_ERROR	special file creation error
A018	CANNOT_DEL_NON_EMPTY	cannot delete non-empty dir
A019	CANNOT_WRITE_DANGLING_SYMLINK	cannot write dangling (dead) link
AFFD	MISS_LAST_MODIFIED	the file update confirmation request miss
AFFE	FILE_OUT_OF_DOC_ROOT	file access outside the document root

AFFF	FILE_SIZE_OVER_LIMIT	the file size exceeded the maximum
B001	BUSY	the server is busy
B002	CONNECT_FAILED	the connection failed
B003	REFUSED	the server denied
B802	OP_NOT_PERMITTED	operation not permitted
BFF3	SESS_ALREADY_SHUTDOWN	session already shutdown
BFF4	SESS_COLLISION	session conflicted
BFF5	SCH_BIND_FAILED	secondary channel binding error
BFF6	SESS_ID_NOT_FOUND	session identifier unknown
BFF8	INCOMPATIBLE_FEATURE	incompatible feature
BFF9	RL_ABORT	aborted by the resource limits
BFFA	INCOMPATIBLE_PROTO_VERSION	the protocol is incompatible
BFFB	SETUP_FAILURE	the setup failed
BFFC	NET_UNAVAIL	the network is unavailable
BFFD	DISK_FULL	the disk is full
BFFE	SESS_NOT_FOUND	the session was not found
BFFF	PROTO_ERROR	protocol error
FFFD	GC_ABORT	abortion by GC (the process stops and etc)
FFFE	INTERNAL_ERROR	internal error
FFFF	GENERAL_ERROR	general error

4.4 Signal control

This service (the hcpd daemon) takes care of signals as described below.

The following signals are processed as the signals for service stop.

signal name	description
-------------	-------------

SIGINT	Terminal interruption
SIGTERM	Terminal end

When SIGINT is caught, the service will stop after the completion of the transmission at that time. In comparison, SIGTERM will stop at once by aborting the transmission.

The following signals are processed as the signals for service restart (reload).

signal name	description
SIGHUP	Hung-up
SIGUSR1	USR1 signal

The following signals are ignored.

signal name	description
SIGALRM	Alarm
SIGPIPE	Pipe writing error

Signals other than the above will not be processed (it behaves following the operating system rules).

The signal numbers may differ depending on the platform. Please refer to the operation system manual.

4.5 Application signals

When client commands (such as hcp) and services are executed by privilege separation, applications in the child process can take advantage of this signal and control the following operations.

The following signals are processed as the signals for service abort. The service will stop the processes of the application at that time, free the resources, and stop the process.

signal name	description	Windows
SIGINT	Terminal interruption	○
SIGTERM	Terminal end	○
SIGUSR1	USR1 signal	×

The following signals are processed as the signals for abort signals based on the resource limit. The service will stop the processes of the application at that time, free the resources, and stop the process.

signal name	description	Windows
SIGUSR2	USR2 signal	×
SIGXCPU	CPU limit	×
SIGXFSZ	file size limit	×

The following signals are processed as the signals for releasing resources. Right after releasing as many resources as possible (such as the HpFP socket descriptor and so on) and retransmitting (re-raise), the process will stop.

signal name	description	Windows
SIGHUP	Hung-up	×

Don't use this signal for child processes, which may cause problems on the entire service running (may need to force-quit the service and restart).

The following signals are ignored.

signal name	description	Windows
SIGALRM	Alarm	×
SIGPIPE	Pipe writing error	×

Signals other than these, such as SIGKILL, SIGABORT, and so forth, are not processed (behave following the operation system). Some of the resources may go unavailable (the HpFP socket descriptor and so on).

Don't use this signal for child processes, which may cause problems on the entire service running (may need to force-quit the service and restart).

Signal numbers can be different depending on the platform. Please refer to each operation system manual.

5 Command execution mode

Bytix Archaea tools provide the following two command execution modes for clients.

- Single running mode
- Multiple running mode

Multiple running mode is set by adding “—multi-run” option. When not added, it starts in the single running mode. Multiple running mode is useful when multiple users share the same working directories together simultaneously or running in the background is needed.

How to execute in respective mode and precautions are below.

5.1 Single running mode

This mode is for a single user operating commands sequentially in specific working directories. The command end status is acquired as the same way as the normal commands.

```
--
Example :
(Linux / Mac)
[user@localhost ~]$ hcp src.txt dest.txt
...
[user@localhost ~]$ echo $?
0
(Windows)
C:\Users\user> hcp src.txt dest.txt
...
C:\Users\user> echo %ERRORLEVEL%
0
--
```

When command execution records are not output as standard with the `—hcp-out` option, they are recorded with the following names in the current directory which is truncated each time they are executed.

```
.hcp.out (Linux / Mac)
_hcp.out (Windows)
```

The application path is output as standard by default like below. With `-l` option and the specified file path, it is output in the file specified by the path.

```
2019/11/01 13:33:35 00007fae521a3b80:INFO :Set bandwidth outbound to unlimited since the specified value is over 5Gbps (given limit : 10000000000 bps).
2019/11/01 13:33:35 00007fae521a3b80:INFO :Set bandwidth inbound to unlimited since the specified value is over 5Gbps (given limit : 10000000000 bps).
2019/11/01 13:33:38 00007fae4aa4a700:INFO :A transport timeout monitor was setup (sock=5, _recv). Monitoring the timeout ...
2019/11/01 13:33:38 00007fae4aa4a700:INFO :A transport timeout monitor becomes disabled (sock=5, ret=0, errno=0, _recv).
```

The statistics records (the application statistics and the transport statistics) are recorded with the following names in the current directory, when their destinations are not specified. These records are not truncated.

```
.hcp.statistics.application (Linux / Mac)
.hcp.statistics.transport.tcp (Linux / Mac)
.hcp.statistics.transport.hpfp (Linux / Mac)
_hcp.statistics.application (Windows)
_hcp.statistics.transport.tcp (Windows)
_hcp.statistics.transport.hpfp (Windows)
```

With -L option, the statistics records can be output in the specified directory with the specified prefix.

--

Example :

```
[root@localhost ~]# hcp -L /var/tmp/.hcp.statistics2 ...
// output directory : /var/tmp
// file name prefix : .hcp.statistics2
```

--

5.2 Multiple running mode

This mode is used, when a user share the same working directories simultaneously with other users or a single user operate plural commands simultaneously using the background. The command end status is acquired by the same way as the single running mode or by referring to the EXIT parameter recorded in the result output.

--

Example :

```
[user@localhost ~]$ hcp --multi-run=/var/tmp ...
2019/11/01 14:02:06 00007f35da531b80:INFO :A configuration file (/home/user/.hcp/hcp.conf) was not found. So it was skipped.
2019/11/01 14:02:06 00007f35da531b80:      :Recording on multi-running is configured (ID=hcp.mr.20191101_140206_442.15279, dir=/var/tmp, out=ATR).
2019/11/01 14:02:06 00007f35da531b80:INFO :Set bandwidth outbound to unlimited since the specified value is over 5Gbps (given limit : 10000000000 bps).
2019/11/01 14:02:06 00007f35da531b80:INFO :Set bandwidth inbound to unlimited since the specified value is over 5Gbps (given limit : 10000000000 bps).
Login as:user
Password:
2019/11/01 14:02:09 00007f35d2dd8700:INFO :A transport timeout monitor was setup (sock=5, _recv). Monitoring the timeout ...
2019/11/01 14:02:09 00007f35d2dd8700:INFO :A transport timeout monitor becomes disabled (sock=5, ret=0, errno=0, _recv).
```

```
[user@localhost ~]$ hcp -l hcp.log --multi-run=/var/tmp ...
2019/11/01 14:04:23 00007fb04eac3b80:INFO :A configuration file (/home/user/.hcp/hcp.conf) was not found. So it was skipped.
```

Bytix Archaea tools Command Reference

```
2019/11/01 14:04:23 00007fb04eac3b80:      :Logging on multi-running is co
nfigured (ID=hcp.mr.20191101_140423_458.15318, dir=/var/tmp, path=/var/tm
p/hcp.mr.20191101_140423_458.15318.log).
Login as:user
Password:
[user@localhost ~]$ less /var/tmp/hcp.mr.20191101_140423_458.15318.log
2019/11/01 14:04:23 00007fb04eac3b80:      :Recording on multi-running is
configured (ID=hcp.mr.20191101_140423_458.15318, dir=/var/tmp, out=ATR).
2019/11/01 14:04:23 00007fb04eac3b80:INFO :Set bandwidth outbound to unli
mited since the specified value is over 5Gbps (given limit : 10000000000
bps).
2019/11/01 14:04:23 00007fb04eac3b80:INFO :Set bandwidth inbound to unlim
ited since the specified value is over 5Gbps (given limit : 10000000000 b
ps).
2019/11/01 14:04:26 00007fb04736a700:INFO :A transport timeout monitor wa
s setup (sock=6, _recv). Monitoring the timeout ...

[user@localhost ~]$ cat /var/tmp/hcp.mr.20191101_140423_458.15318.out | g
rep -e EXIT
EXIT 0 REASON 0000
--
```

In this mode, the following lock file is created in the directory specified by the `—` multi-run option on starting to execute the command.

hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.lock

The following records are saved with the file name adding the strings to the prefix (the strings before “.lock”) of this lock file each time the command is executed.

- Application statistics
- Transport statistics
- Result output
- Application log

In this mode, these records are not provided, if exiting with the following error statuses. The exit status can be confirmed by the command line operation, as in Single running mode.

- EXIT_ERROR_LOAD_ARG (181)
- EXIT_ERROR_LOAD_CONF (182)
- EXIT_ERROR_CLI_SETUP_FAILED (189)

When the back ground mode is used, if exiting with the status shown above, confirming the exit status is difficult. Make sure to save the configuration data in advance.

When the command execution record is output to a file according to the `—multi-run` option, it is recorded with the following file name.

```
hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.out
```

When the command `—hcp-out` option is applied, the command execution record is not stored in the file but output as standard.

When the application log is output to a file according to the `—multi-run` option, it is recorded with the following file name.

```
hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.log
```

When the statistics records (application statistics, transport statistics) are output to files according to the `—multi-run` option, they are recorded with the following file names.

```
hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.statistics.application
hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.statistics.transport.tcp
hcp.mr.<YYYYMMDD_hhmmss_msec>.<pid>.statistics.transport.hfpf
```

6 Server backward compatibility conditions

condition to use	available server versions
Authentication with keys registered in key agent (even if keys not specified at IdentityFile)	1.5.4 or later
Connect to servers using NFS mount as home with <code>root_squash</code> option	1.5.4 or later
Authentication with ECDSA/Ed25519 keys	1.5
Authentication with keys registered in key agent (if keys specified at IdentityFile)	1.5
hln target relative path	1.4.3 or later, 1.3.4 or later
hcp -H option	1.4.3 or later, 1.3.4 or later
hrm single path use, other commands rather than hcp/hsync	1.3 or later, 1.2.4 or later
hcp	1.3 or later
hsync	1.4, 1.3.1 or later
hcp <code>—mcd=1</code> set and no options to read from devices like <code>—reading-dev</code> set	1.2.4 or later

hsync —mcd=1 set and no options to read from devices like —reading-dev set	1.2.7 or later
--	----------------

7 Bytix Archaea tools restriction lists

name	limitation
the maximum value on each configuration	up to 8
the maximum number of characters of 1 line on each configuration	256
the maximum number of error message letters on each configuration	1024
the maximum number of DocPoint definition	up to 10 definitions
the maximum number of user name	256
the maximum number of passwd	256
the maximum file size	the maximum number of 8EiB unsigned 64 bit integer
the maximum characters of file path	2048 characters
invalid characters for file path such as non printable characters, OS incompati	ble characters, newline code and so on
the number of file cache entries100000entries	
Number of results to output for files waiting to be processed	up to 1000 results
Number of supplemental groups for privilege separation	up to 1000

The length of a file path is different depending on the platform of the file system. In general, 260 letters including drive letter can be used on Windows.

8 Notation

Supported OS and names noted as the defaults, configurations or examples on each OS follow the rules below.

The following each OS and its version are shown by the label noted in brackets.

- Red Hat Enterprise Linux 7 / CentOS 7 (RHEL7)
- Red Hat Enterprise Linux 8 / AlmaLinux 8 (RHEL8)
- Red Hat Enterprise Linux 9 / AlmaLinux 9 (RHEL9)

- SUSE Linux Enterprise 15 SP3 / openSUSE Leap 15.3 (SLE15.3)
- SUSE Linux Enterprise 15 SP4 / openSUSE Leap 15.4 (SLE15.4)
- SUSE Linux Enterprise 15 SP5 / openSUSE Leap 15.5 (SLE15.5)
- Ubuntu 20.04 LTS / Debian 11 (Ubuntu20.04)
- Ubuntu 22.04 LTS / Debian 12 (Ubuntu22.04)
- Ubuntu 24.04 LTS / Debian 13 (Ubuntu24.04)
- Raspberry Pi OS 9 (RaspiOS9)
- Raspberry Pi OS 11 (RaspiOS11)
- Windows 10 (Win10)
- Windows 11 (Win11)
- Windows Server 2012 R2 (WinServ2012R2)
- Windows Server 2016 (WinServ2016)
- Windows Server 2019 (WinServ2019)
- macOS Catalina (MacCatalina)
- macOS Big Sur (MacBigSur)
- macOS Monterey (MacMonterey)
- macOS Ventura (MacVentura)
- macOS Sonoma (MacSonoma)

These OSs are shown as a group by the label noted in brackets.

- RHEL7 / RHEL8 / RHEL9 (RHEL)
- SLE15.3 / SLE15.4 / SLE15.5 (SLE)
- Ubuntu20.04 / Ubuntu22.04 / Ubuntu24.04 (Debian)
- RaspiOS9 / RaspiOS11 (RaspiOS)
- Win10 / Win11 / WinServ2012R2 / WinServ2016 / WinServ2019 (Windows)
- MacCatalina / MacBigSur / MacMonterey / MacVentura / MacSonoma (Mac)

Distribution groups of Linux are shown by the label noted in brackets.

- RHEL / SLE / Debian / RaspiOS (Linux)
- RHEL / SLE / Debian (Linux.x86)

9 revision history

revision date	revision point
2025/11/04	Updated version description of HpFP.
2025/10/15	A command parameter description is modified.
2025/02/13	Setting items were added and platform information was modified.

2024/10/18	Command parameter descriptions are added or modified. Updated the platform information.
2024/06/27	Command parameter descriptions and configuration descriptions are added. Update Notation.
2024/04/22	Command parameter descriptions and configuration descriptions are added. Some wrong descriptions are fixed.
2023/12/21	Command parameter descriptions and configuration descriptions are added.
2023/10/20	Edit configuration descriptions.
2023/09/14	Configuration descriptions are added. ECDSA/Ed25519, some descriptions about RHEL7 are deleted.
2023/08/23	Command parameter descriptions and configuration descriptions are added.
2023/08/02	ECDSA/Ed25519, some descriptions about RHEL7 are added.
2023/07/28	Command parameter descriptions and configuration descriptions are added.
2023/05/20	Command parameter descriptions are added, notation updated.
2023/02/28	Setting items, command parameter descriptions are added.
2022/12/07	Description of supported PuTTY key versions. Added and updated description around AuthorizedKeys. Updated the platform information.
2022/10/20	Description of server backward compatibility was modified.
2022/10/13	Description of new algorithm of AES/GCM and xxHash were added. Updated the platform information. Fixed some statements.
2022/07/12	Descriptions of configuration and hsync were added. Some statements fixed and translation made from the Japanese.
2021/11/29	Descriptions of configuration, hsync, hchmod and hchown were added. Command helps were edited.
2021/09/10	Descriptions of POSIX user and group access control and others were added.
2021/05/16	Default value's descriptions were modified. Descriptions of configuration and application statistics were added.
2021/04/23	Fixed wrong descriptions of default values.
2021/04/18	Descriptions of multiple connections per session and WebSocket were added.
2021/02/09	Setting items, command parameter descriptions are added. Examples are revised.

Bytix Archaea tools Command Reference

2020/09/03	Defaults in Linux, format description, archivecheck were added and reserved descriptions were revised.
2020/07/30	UseProperCopyAndSync explanation were revised.
2020/07/21	Reserved descriptions, FileOperationLog explanation were revised. Signal explanations were added.
2020/05/15	Configuration explanations, and error codes were added.
2020/04/23	MAC disable explanation were added.
2020/02/10	FileOperationLog explanation were added.
2019/12/16	Home directory check explanation was added.
2019/12/11	Log rotation explanation was added. File path length was annotated.
2019/11/12	Errors in writing were corrected. Public key search rules were annotated.
2019/11/05	Output numbers were revised.
2019/11/01	Errors in writing were corrected. Descriptions were revised. Configuration explanations were added.
2019/06/07	Commands descriptions were added and revised and reason codes were added
2019/04/26	Users sample descriptions were revised
2019/04/25	Option descriptions were added and revised
2019/02/01	Incorrect descriptions for Option were corrected
2019/01/30	Incorrect descriptions were corrected and descriptions for include configurations were added.
2019/01/29	Incorrect descriptions were corrected.
2019/01/21	The specifications on the server key file path were changed.
2019/01/20	Some commands were added. Descriptions for Windows version were added.
2018/07/30	Application statistics expressions were changed. output examples were changed.
2018/07/30	End status and reason codes were changed.