

NEC Ultra-high-speed Data Transfer System Manual

Table of Contents

Preface.....	5
Disclaimer	6
Purpose of This Manual	6
Applicable Version	6
Intended Audience.....	6
Prerequisites	6
Organization of This Manual.....	7
Notation.....	7
1 Overview.....	9
1.1 What's NEC Ultra-high-speed Data Transfer System	10
1.2 Recommended Usages	10
1.3 Characteristics.....	10
1.4 List of Functions	11
1.5 Function Detail (Fast and Highly Efficient Communication)	13
1.6 Function Detail (Realization of Secure Data Transfer)	23
1.7 Function Detail (for Supporting System Operation and Management).....	31
1.8 List of Commands Provided	38
1.9 Supported Platforms	39
1.10 Hardware Requirements.....	39
1.11 Software Requirements	40
1.12 Network Requirements.....	41
2 Server Setup	42
2.1 Red Hat Enterprise Linux (RHEL)	43
2.2 RPM Install the software into a non-default place.....	44
2.3 RPM Install the software by non-privileged users	45
2.4 How to use hcpd by users without privilege.....	47
3 Server Command	49
3.1 Server Command (hcpd)	50
4 Server Configuration.....	65
4.1 Server Setting Files	66
4.2 Server Setting Items.....	66

5 Client Setup	148
5.1 Red Hat Enterprise Linux (RHEL)	149
5.2 RPM Install the software into a non-default place.....	150
5.3 RPM Install the software by non-privileged users	151
5.4 Confirm if It Works After Installation	152
6 Client Commands	154
6.1 Client Command (hcp).....	155
6.2 Client Command (hsync)	203
6.3 Client Command (hrm)	250
6.4 Client Command (hcp-ls).....	259
6.5 Client Command (hmkdir)	266
6.6 Client Command (hpwd)	272
6.7 Client Command (hmv).....	277
6.8 Client Command (hln).....	285
6.9 Client Command (hchmod)	295
6.10 Client Command (hchown).....	302
6.11 Command Execution Mode	310
7 Client Configuration.....	315
7.1 Client Setting Files	316
7.2 Client Common Command Setting Items.....	317
7.3 Client Command Setting Items (hcp).....	349
7.4 Client Command Setting Items (hsync)	355
7.5 Client Command Setting Items (hrm)	356
7.6 Client Command Setting Items (hcp-ls).....	357
7.7 Client Command Setting Items (hmkdir)	357
7.8 Client Command Setting Items (hpwd).....	358
7.9 Client Command Setting Items (hmv).....	358
7.10 Client Command Setting Items (hln).....	359
7.11 Client Command Setting Items (hchmod)	359
7.12 Client Command Setting Items (hchown).....	359
8 Error Codes and Signals.....	361
8.1 Command End Status	362
8.2 Configuration File Error Codes	363
8.3 File Processing Code	364
8.4 Application Signals	367
8.5 Signal Control.....	368

9 Statictics Information 370

 9.1 Application Statistics 371

 9.2 Transport Statistics 375

 9.3 System Statistics 378

A Appendix 381

 A.1 Notes..... 382

 A.2 NEC Ultra-high-speed Data Transfer System Restriction Lists..... 386

 A.3 Trademarks 386

 A.4 Revision History 387

 A.5 Document Information 387

Preface

Disclaimer

Every effort has been made to ensure the accuracy of the contents of this manual. However, NEC does not guarantee their completeness, accuracy, or usefulness.

The contents of this manual are subject to change without notice due to improvements or for other reasons.

NEC shall not be liable for any damages arising from the use of, or inability to use, the contents of this manual.

Purpose of This Manual

The purpose of this manual is to provide the information required for the installation, configuration, use, and operation of the NEC Ultra-high-speed Data Transfer System.

This manual describes the overview, operating environment, setup procedures, commands, configuration files, error codes and signals, statistical information, precautions, and restrictions for the server software and the client software that constitutes the NEC Ultra-high-speed Data Transfer System.

Applicable Version

This manual applies to NEC Ultra-high-speed Data Transfer System Version 1.0.1.

Intended Audience

This manual is intended for the following users involved in the installation, configuration, operation, or use of the NEC Ultra-high-speed Data Transfer System:

- Users who install NEC Ultra-high-speed Data Transfer System and perform its initial setup
- Users responsible for configuring, maintaining, and operating the machine environment in which NEC Ultra-high-speed Data Transfer System is installed
- Users who use the various commands of the client software for the NEC Ultra-high-speed Data Transfer System
- Users who refer to command specifications, configuration settings, restrictions, and troubleshooting information

Prerequisites

This manual assumes that readers have basic knowledge of the following:

- Basic OS operations for using the server software and client software of the NEC Ultra-high-speed Data Transfer System
- Command-line operations
- Handling of files and directories

In addition, users responsible for server installation and operation are expected to have basic knowledge of the following:

- Networking
- System administration

Organization of This Manual

The organization of this manual is shown below.

Chapter	Description
Preface	Describes the disclaimer, the purpose, supported version, intended audience, prerequisites and notation used in this manual.
Overview	Describes the overview, use cases, features, functions, provided commands, supported environments, and various requirements of the NEC Ultra-high-speed Data Transfer System.
Server Setup	Describes how to install and perform the initial setup of the server software.
Server Commands	Describes the functions and usage of the server command (<code>hcpd</code>).
Server Configuration	Describes the server configuration files and configuration items.
Client Setup	Describes how to install the client software and verify its operation.
Client Commands	Describes the functions, usage, and execution modes of each client command.
Client Configuration	Describes the client configuration files and the configuration items for each command.
Error Codes and Signals	Describes exit statuses, error codes, reason codes, and signal handling.
Statistical Information	Describes the contents of various types of statistical information.
Appendix	Provides usage notes and restrictions.

Notation

< `parameter` >

This represents an essential parameter. You need to enter it on command lines.

[< `parameter` >]

This represents an optional parameter. You can omit it on command lines.

1 Overview

1.1 What's NEC Ultra-high-speed Data Transfer System

NEC Ultra-high-speed Data Transfer System is an innovative file transmission toolset that can transfer and synchronize huge files and also a large number of small files securely and very efficiently.

The software realizes fast file transfers even in LFN (Long Fat Network) or to overseas bases in poor networks.

The software includes practical functions widely used in the Unix platform, such as the SCP file transfer, the rsync synchronization, SSH-like secure communication, and high-performance transmission.

1.2 Recommended Usages

The NEC Ultra-high-speed Data Transfer System will make highly useful effects in different cases where you have to make missions on R&D and business.

- Utilizing on the HPC (High Performance Computing) environment.
- Moving massive data from on-premises to the cloud more efficiently.
- Rapidly sharing files with overseas bases.
- File transfer making the most of a wide area/broadband network over 1 Gbps
- making file backups onto remote sites for BCP (Business Continuity Plan).
- Fast transfer of huge files between data centers.
- Efficient use of cloud environments
- Solving issues about communication performance on current systems.

1.3 Characteristics

1.3.1 Ultimately Fast File Transfer

NEC Ultra-high-speed Data Transfer System can achieve the ultimate in high-speed file transfers in any environment.

Proprietary communication engine "HpFP2" (High-performance and Flexible Protocol ver.2) enables significantly high-speed communication.

HpFP2 is a technology to maximally enhance the line usage efficiency with an innovative transmission control on the UDP layer by keeping the interface compatible with TCP sockets.

HpFP2 includes different effective controls to solve typical issues on the UDP communications, such as effective retransmission control, congestion control, transmission control, and flow control, which realizes remarkably high transmission efficiencies without significant drops in the communication speed in unstable or high latency network environments.

It can also realize that wide band networks over 1Gbps for HPC achieve high- speed file transfer, making the most of the bandwidth.

1.3.2 Effective Bundling Transfer of Many Files

The NEC Ultra-high-speed Data Transfer System realize effective file transfer for different sizes of files from small to large.

The most difficult case for FTP(File Transfer Protocol) widely used in transferring files, is to transfer many small files collectively.

On the other hand, the NEC Ultra-high-speed Data Transfer System efficiently and collectively process files with a memory buffer assigned for each one, which results in greatly shortening the processing time. The more files, the more effective.

- It realizes highly effective file transfer of many small files [Asynchronous Incremental File Transfer]
- It realizes super high speed parallel file transfer [Asynchronous Multi-Connection Parallel File Transfer]

1.4 List of Functions

The NEC Ultra-high-speed Data Transfer System include the following functions.

Category	Function	Description
Fast and Highly Efficient Communication	Transport Selection	Single/multiple connection, TCP/UDP/HTTP selectable
	Multiple files batch transfer	file list/regular expression/wildcards selectable
	Congestion Control	fair/fast-start/modest/aggressive selectable
	Communication Data Compression Function	ZIP format compression by packet supported
	Data Flow Control	tuning available by data flow controls - bandwidth shaping - file lock - temporary file save - data buffer size configuration - file size limitation to transfer - protocol message block size tuning - disk I/O throughput shaping
Security	String Encoding	Transfer encode negotiation and host character encoding supported
	Authentication	PAM, Public key available
	Encryption	AES(256 bit/192 bit/128 bit) block cipher, CBC/CTR/GCM modes, communication message encryption, communication security negotiation, etc.
	Access Control	Privilege separation, access control list, admission control, document points, etc.
	Data Integrity Validation	Detection of data errors occurring in networks
System Operation Support	Resume transfers	When a file transfer is unexpectedly aborted, it resumes where it left off.
	Monitoring Function	Timeout control, start in the foreground mode, etc.
	Performance Evaluation	Protocol performance evaluation mode, storage I/O performance evaluation mode
	Log Management	Log level (info/warn/error), log data (different kinds of statistics), output file (Syslog/specified file) selectable
	Software Information	Display software version, configuration, command parameters and, help

Category	Function	Description
	System operating environment settings	Specify configuration file path, CPU thread limitation, application integration function, etc.
	File and Directory Manipulation	Clients can remotely operate (create/delete/move/display/list) files, directories, and links on a server

1.5 Function Detail (Fast and Highly Efficient Communication)

1.5.1 Transport Selection

Various transmission methods are available to suit different environments and purposes by combining the following connection methods and protocols.

Connecting Method

- Single Connection Mode
- Multiple Connection Mode

Available Protocols

- TCP
- HpFP (in UDP transport, proprietary protocol)

In Single Connection Mode, the software creates a session for a single connection.

In Multiple Connection Mode, it creates multiple sessions for a single connection. This mode is useful for making file transfers on wide band networks over 10Gbps up to 100Gbps by processing multiple sessions simultaneously across multiple CPU cores since the performance of the single connection is up to 20Gbps or less.

Selectable Connection Methods and Suitable Environments

Connection method	Protocol	Description	Effective environment
Single-connection	TCP	General TCP communication	Environments having low latency and low packet loss
	HpFP (UDP)	proprietary communication method	Environments having high latency and high packet loss
Multiple-connection	TCP	General TCP communication	Environments having both of latency and low packet loss or broadband networks
	HpFP (UDP)	proprietary communication method	Environments having both of high latency and high packet loss or broadband networks

* Please see the "Considerations on performance characteristics" in "Notes" for performance tuning of communication.

Related Options

Command	Short Name	Option Name	Description
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hcho-wn		hpfp	Use the HpFP protocol
		udp	Use the UDP(HpFP) protocol (bi-port form, deprecated)
hcp/hsync		mcd	Set the number of maximum connections per session

Related Configurations

Category	Configuration Name	Description
Server Configuration	TCPListenAddress	TCP service listen address setting
	HPFPListenAddress	HpFP service listen address
	UDPListenAddress	HpFP service listen address (bi-port type, deprecated)
	ListenServiceBonding	Listen service bonding

1.5.2 Transfer Bundle of Files

NEC Ultra-high-speed Data Transfer System can transfer a bundle of files by specifying file list or type to send together.

Related Options

Command	Short Name	Option Name	Description
hcp	g	regex	File names recognized as regular expressions (but not in wild - card manner)
hcp	f	source-file	Source file list

1.5.3 Congestion Control

The following congestion control modes are prepared for each environment and purpose of use.

Congestion Control Mode	Abbreviation	Description
Fair Mode	F	fairly shares the bandwidth with other protocols such as TCP/IP.
Modest Mode	M	emits packets only when the bandwidth has enough capacity to send.
Fair Fast-Start Mode	S	communicates at high speed initially but behaves as the fair mode after that.
Aggressive Mode	A	accelerates the throughput aggressively up to the maximum line bandwidth.

Aggressive Mode is an experimental function.

When processing load increases by communications over 10 Gbps, the performance may drop by packet loss. Especially when using the multi-channel function, the CPU core is not evenly allocated by the RSS function of NIC, which may cause unstable throughput. In those cases, Fair mode is recommended.

Related Options

Command	Short Name	Option Name	Description
hcp/hsync/hrm/hcp- ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		hpfp- cong	Congestion control modes in the HpFP protocol

1.5.4 Communication Data Compression Function

Transfer data can be compressed by packet, which can shorten transmission time. This function works effectively in environments where data transmission speed is slower than the data compression speed. The compression level can be also chosen.

Related Options

Command	Short Name	Option Name	Description
hcp	z	compress	Compress transferred data blocks

Related Configurations

Category	Configuration Name	Description
Server Configuration	HeaderCompress	Header compression (reserved)
	ContentCompress	Content compression (reserved)
Client Common Configuration	CompressLevel	Compress level
	HeaderCompress	Header compression
	ContentCompress	Content compression

1.5.5 Data Flow Control

Various data flow controls allow for the best tuning to each environment.

- Bandwidth control

Shaping bandwidth makes the data-transfer rate stable.

This function limits the bandwidth between the TCP/HPFP(UDP) layer and the application layer. Therefore, the application layer gets limited. However, the Communication buffer and the transmission control on the transport layer are not affected.

Servers can set the configuration both on the system and on each connection.

With over 10Gbps in each setting, the bandwidth gets unlimited, which results in no shaping.

Related Options

Command	Short Name	Option Name	Description
hsync		bwlimit	Limit socket I/O bandwidth

Related Configurations

Category	Configuration Name	Description
Server Configuration	MaxTotalReceiveRate	Maximum total receiving rate (entire system)
	MaxTotalSendRate	Maximum total sending rate (entire system)
	MaxReceiveRatePerConnection	Maximum receiving rate (per connection)
	MaxSendRatePerConnection	Maximum sending rate (per connection)
Client Common Configuration	MaxReceiveRate	Max receiving rate (by session)
	MaxSendRate	Max sending rate (by session)

- File lock

This is a file lock function that the file gets locked and inaccessible while the file data is being read or written.

File lock is a system that temporarily confines the users and processes that can access to files.

In the process, after the file gets locked, the file is read or written. Advisory lock is supported on the Linux platform. This function is available between this software and also other software that uses the same file lock system.

When a hung-up happens in the network file system, such as NFS(Network File System), or an error occurs when getting a file lock, this function has to be disabled. It is also requested to make sure the destination in the hcp commands is not input double.

And configurations of the number of maximum trials and the interval time on the file lock are also provided.

Related Configurations

Category	Configuration Name	Description
Server Configuration	FileLock	Use file lock
	FileLockTrials	Number of trials to lock files
	FileLockTrialInterval	The trial interval (in seconds)
Client Common Configuration	FileLock	Use file lock
	FileLockTrials	Number of trials to lock files
	FileLockTrialInterval	The trial interval (in seconds)

- Creating Temporary File to Save (atomically file saving)

This function performs a two-step file saving using a temporary file on writing transferred data to a file.

It's for writing data to files in safety.

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.

The overwrite-als-temp-file option of the hcp command 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.

The configuration of a threshold in file size to enable saving files atomically is provided. The saving atomically does not cover files under the threshold. "0 bytes" means all files are covered.

Related Options

Command	Short Name	Option Name	Description
hcp		overwrite-als-temp-file	Atomically overwrite a temporary file

Related Configurations

Category	Configuration Name	Description
Server Configuration	AtomicLikeSaving	Atomically file saving
	AtomicLikeSavingThreshold	Threshold for atomically file saving
	AtomicLikeSavingRejectOverwriteRequest	Reject requests to overwriting temporary files which already exist when atomically file saving
Client Configuration (hcp)	AtomicLikeSaving	Atomically file saving
	AtomicLikeSavingThreshold	Threshold for atomically file saving

- Data Buffer Configuration

NEC Ultra-high-speed Data Transfer System setups a data buffer in a part of the general main memory for buffering transferred data. This is a function to configure size of the data buffer.

Its configuration on the server side includes a total size on the system and a size per session.

And configurations of a sending buffer size on TCP (TCPServiceSocketSendBuffer) and an extension buffer size of HpFP (UDPServiceExtensionBufferSize) are also provided.

You need the option of TCPServiceSocketSendBuffer to make a performance tuning of TCP on 100G environment. No need to use in ordinary cases.

Each HpFP transport session extends a buffer holding transferred data up to a size specified by hpfp_sndbuf or hpfp_rcvbuf on HPFPListenAddress or UDPListenAddress. '0' indicates disabling this buffer extension and the initial size before extending is 1MB.

Workarounds when a process is killed by Linux OOM (Out Of Memory) Killer

As an OS mechanism, Linux monitors memory consumption trends of processes and terminates (KILL signal) processes which run out of memory. When you set the following buffer size options, e.g, MaxTotalBufferSize or MaxBufferSize, in this software to values large than system memory, Linux OOM Killer might kill the process. For fixing it you have to specify smaller buffer size values for the options or extending the system memory.

Related Options

Command	Short Name	Option Name	Description
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchow		hpfp-sndbuf	Set the sending buffer size for the HpFP protocol
n		hpfp-rcvbuf	Set the receiving buffer size for the HpFP protocol

Related Configurations

Category	Configuration Name	Description
Server Configuration	HPFPListenAddress	HpFP service listen address
	UDPListenAddress	HpFP service listen address (bi-port type, deprecated)
	MaxTotalBufferSize	Maximum buffer allocation size (entire system)
	MaxBufferSizePerConnection	Maximum buffer allocation size (per connection)
	TCPServiceSocketSendBuffer	TCP sending buffer
	UDPServiceExtensionBufferSize	HpFP service extension buffer size
Client Common Configuration	MaxBufferSize	Maximum buffer allocation size
	UDPTTransportExtensionBufferSize	HpFP transport buffer size extension
	TCPTransportSocketSendBuffer	TCP sending buffer

- Limitation File Size to Transfer

This is a function to set maximum sizes of files to transfer.

Related Configurations

Category	Configuration Name	Description
Server Configuration	MaxReceiveFileSize	Maximum receiving file size
	MaxSendFileSize	Maximum sending file size
Client Common Configuration	MaxReceiveFileSize	Maximum receiving file size
	MaxSendFileSize	Maximum sending file size

- Communication Message Size Control

This is a function to configure sizes of transfer data blocks made from payloads of files.

NEC Ultra-high-speed Data Transfer System evaluates consumption of bandwidth after starting transfers. And it increases and decreases sizes of header blocks including messages, e.g. file requests, and content blocks including a payload data of a file subject to the evaluation.

You can set options for that mechanisms, InitHeaderBlockSize for a initial size of the header blocks, InitContentBlockSize for a initial size of the content blocks, MaxHeaderBlock for a maximum size of the header blocks and MaxContentBlockSize for a maximum size of the content blocks.

And a configuration of MSS (Maximum Segment Size) for HpFP protocol is also provided for the frame size control on transport.

Related Options

Command	Short Name	Option Name	Description
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		hfp-mss	Set MSS for the HpFP protocol

Related Configurations

Category	Configuration Name	Description
Server Configuration	InitHeaderBlockSize	Initial header block size
	InitContentBlockSize	Initial content block size
	MaxHeaderBlockSize	Maximum header block size
	MaxContentBlockSize	Maximum content block size
	MaxRequestFileEntryAtOnce	Max file entry request
Client Common Configuration	InitHeaderBlockSize	Initial header block size
	InitContentBlockSize	Initial content block size
	MaxHeaderBlockSize	Maximum header block size
	MaxContentBlockSize	Maximum content block size
	MaxRequestFileEntryAtOnce	Max file entry request

• Disk I/O Speed Control

This is a function to set maximum speeds of writing data to a disk and reading from it on file transfers.

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.

Related Configurations

Category	Configuration Name	Description
Server Configuration	MaxReadRatePerConnection	Disk I/O reading rate per session
	MaxWriteRatePerConnection	Disk I/O writing rate per session
Client Configuration (hcp)	MaxReadRate	Disk I/O reading rate per session
	MaxWriteRate	Disk I/O writing rate per session

1.5.6 String Code Conversion

This is a function to avoid character corruption by converting strings among string codes.

- Transport Character Encoding Negotiation

This is a function to determine a character encoding for strings to be transferred over networks.

Encodings to use are supposed to be specified in configuration files of the client and server. The encodings will be applied to strings, e.g. file paths exchanged between the server and client. NEC Ultra-high-speed Data Transfer System determines an actual encoding to use by a way that it compares configurations of the server and client and determines an encoding defined in common.

Related Configurations

Category	Configuration Name	Description
Server Configuration	TransportCharEncoding	Transport character encoding
Client Common Configuration	TransportCharEncoding	Transport character encoding

- Host Character Encoding Support

This is a function to convert strings in a string code on the operating system (host) to strings in another string code on the software processing of NEC Ultra-high-speed Data Transfer System.

This function avoids character corruption by setting a string code used on the host operating system. For example, that string conversion will be applied to file paths to convert them to the software internal representation.

Related Configurations

Category	Configuration Name	Description
Server Configuration	HostEncoding	Host character encoding
Client Common Configuration	HostEncoding	Host character encoding

1.6 Function Detail (Realization of Secure Data Transfer)

For secure usage, NEC Ultra-high-speed Data Transfer System provides functions that ensure confidentiality and integrity of transferred data and authenticate it to identify correct peers of communication.

- Use public key technologies and authenticate peers of communication by them.
- The international standard of AES (Advanced Encryption Standard) protects transferred data to prevent confidential information from being disclosed. In addition, AES encryption/decryption uses the CPU-integrated AES-NI (Advanced Encryption Standard New Instructions), achieving both security and high performance.
- Privilege separation and access control list function realizes an appropriate access control.
- Payload validation detects data errors over networks.
- Transfer resuming makes efficient transfer even if unexpected transfer aborting happens.

1.6.1 Authentication

NEC Ultra-high-speed Data Transfer System supports the following standard authentication functions.

- PAM (Pluggable Authentication Modules) authentication
- Public key authentication

And it provides the following configurations about its authentication functions.

Type	Configuration Item	Description
PAM (Pluggable Authentication Module) (Linux)	PAMAuthentication	PAM configuration
Public key authentication	PubkeyAuthentication	Public key authentication configuration

PAM authentication of NEC Ultra-high-speed Data Transfer System also supports LDAP (Lightweight Directory Access Protocol) authentication if the deployment environment can provide it for logind, sshd or other services. In that case, the NEC Ultra-high-speed Data Transfer System performs the LDAP authentication using the configuration file of `/etc/pam.d/hcpd`.

Related Options

Command	Short Name	Option Name	Description
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		no-agent	Don't use agent
		ident-select	Select identity
		user	Specify username in advance
		password	Specify password in advance

Related Configurations

Category	Configuration Name	Description
Server Configuration	PAMAuthentication	PAM (Pluggable Authentication Module) authentication
	PubkeyAuthentication	Public key authentication
	AuthorizedKeysSearchDir	Specify directory for searching public keys (Public key auth)
	AuthorizedKeysFile	Specify file for finding a public key (Public key auth)
	AuthorizedKeysCommand	Specify command for finding a public key (Public key auth)
	AuthorizedKeysCommand User	Specify user to run the command (Public key auth)
	AllowUsers	Specify user name pattern to allow login
	AllowGroups	Specify group name pattern to allow login
	DenyUsers	Specify user name pattern to deny login
	DenyGroups	Specify group name pattern to deny login
Client Configuration	PAMAuthentication	PAM (Pluggable Authentication Module) authentication
	PubkeyAuthentication	Public key authentication
	IdentitySearchDir	Specify directory for searching private keys (Public key auth)
	IdentityFile	Specify file for finding a private key (Public key auth)
	PubkeyAuthenticationPrior	Configure priority of Public key authentication

1.6.1.1 Utilization of Public Key Technologies

NEC Ultra-high-speed Data Transfer System use public key technologies to make secure communication with peers.

The tools support the following algorithms and file formats of private keys and public keys for the secure communication.

The algorithms for the keys are,

- RSA
- ECDSA nistp256, nistp384, nistp521
- Ed25519

And the file formats for the keys are,

- PKCS1
- PKCS8
- OpenSSH ver.1
- PuTTY ver.2 and ver.3

1.6.2 Encryption

It is important to encrypt transferred data when you make transfer of files over networks.

Encryption is to encode data to another form which any third person cannot read. It reduces risks that data is disclosed by their wiretapping.

NEC Ultra-high-speed Data Transfer System provides communication security like SSH/TLS. You don't have to make any configuration for that security as usual. Encryption is enabled by default. However, you can change that configuration on servers and clients to change an encryption algorithm that will be used between them.

- Communication Message Encryption

This is a function to encrypt messages transferred between a client and a server.

In NEC Ultra-high-speed Data Transfer System, you can make configuration of encryption algorithms for encrypting transferred messages and digest algorithms for validating that messages and file payloads. Negotiation of configurations on a client and a server determines a set of algorithms that will be used on actual communication.

Related Configuration

Category	Configuration Name	Description
Server Configuration	AcceptableCryptMethod	Encryption method for message communication
	AcceptableDigestMethod	Digest method for validation of message and file data
	RequireDataIntegrityChecking	Setting requirement of MAC (Message Authentication Code)
Client Common Configuration	AcceptableCryptMethod	Encryption method for message communication
	AcceptableDigestMethod	Digest method for validation of message and file data
	DisableDataIntegrityChecking	Disable MAC or not
	AcceptDataIntegrityCheckingOnRejection	Acceptance of rejection for disabling MAC

- Communication Security Negotiation

This is a function to negotiate a security of communication method between a client and a server.

NEC Ultra-high-speed Data Transfer System provides verification of the authenticity of the communicating server by the server authentication based on public key technology.

A private key for each server authentication will be loaded from the following path in default.

/etc/hcp/key/server.key (Linux.x86)

When a public key exists and the file name adds ".pub" to the name of the private key, the server use the keys as a pair for the server authentication.

Related Configuration

Category	Configuration Name	Description
	ServerKeyFile	Server key path for the server authentication
	StrictHostKeyChecking	Server host key's acceptance policy configuration

1.6.3 Access Control

NEC Ultra-high-speed Data Transfer System provides the following functions to give appropriate access rights authenticated users.

- Privilege Separation

- ACL (Access Control List)
- Admission Control
- Document Points

Related Configuration

Category	Configuration Name	Description
Server Configuration	UserDirectoryFallbackAvailable	Fallback control from user home (for backward compatibility)
	RejectOnUserHomeDirectoryNotFoundFound	Access rejection when a directory of user home is not found

- Privilege Separation

This is a function to separate access rights of users from the privilege of root to make safe usage on the users subject its rights.

NEC Ultra-high-speed Data Transfer System configures privilege separation on a server for its client sessions. Under the privilege separation working, processing in each client session on the server works on a process separated from another process of the server waiting for clients and having the root privilege as usual. On the client process separated from the waiting one, some access rights subject to UID/GID and supplemental groups determined from authentication results will be applied to each processing.

If you disable the privilege separation, the client sessions works under the access rights of Linux daemon running.

Related Configuration

Category	Configuration Name	Description
Server Configuration	UsePrivilegeSeparation	Set privilege separation
	PrivilegeSeparationMinimumUID	Minimum UID applicable for privilege separated sessions
	PrivilegeSeparationMinimumGID	Minimum GID applicable for privilege separated sessions
	PrivilegeSeparationUser	Default user on privilege separation (applied when any user is not determined)
	PrivilegeSeparationUmask	Umask on privilege separation for authenticated users
	PrivilegeSeparationUmaskAnonymous	Umask on privilege separation for anonymous
	ApplyUserPermission	Apply user's access rights to file permissions on destination (not on privilege separation)
	NoSupplementalGroupInPrivilegeSeparation	Disable supplemental groups

- ACL (Access Control List)

This is a function to control accesses from clients based on network features subject to access control lists.

On NEC Ultra-high-speed Data Transfer System, the function also provides specification of congestion control of HpFP for the accept rules.

Related Configuration

Category	Configuration Name	Description
Server Configuration	AccessList	Define ACL (Access Control List)
	Allow	Define Allow rules on ACL
	Deny	Define Deny rules on ACL

- Admission Control

This is a function to limit number of connections working at the same time to control and save server resources, e.g. bandwidth, memory and CPU, for communication.

Related Configuration

Category	Configuration Name	Description
Server Configuration	MaxTotalConnection	Limit of connections (total)
	MaxTcpConnection	Limit of TCP connections
	MaxUdpConnection	Limit of UDP (HpFP) connections
	MaxConnectionPerUser	Limit of connections each user
	MaxConnectionPerSec	Limit of connections to accept each second

- Document Points

This is a function to configure areas on the server file system to which clients are available to access. This function is defined by NEC Ultra-high-speed Data Transfer System and is configured on its servers. The function provides controls of reading, writing, overwriting and deleting around files and directories to allow or deny that operations.

Related Configuration

Category	Configuration Name	Description
Server Configuration	DocPoint	Define a document point
	DocPath	Specify a path on file system on the document point
	Homelsolation	Set user home isolation
	PermitAccessRead	Set reading access configuration
	PermitAccessWrite	Set writing access configuration
	PermitAccessOverwrite	Set overwriting access configuration
	PermitAccessDelete	Set deleting access configuration
	PermitAccessRandomRead	Set reading in random access configuration (Reserved)
	PermitAccessRandomWrite	Set writing in random access configuration (Reserved)

1.6.4 Data Integrity Validation

This is a function to detect unexpected problem over networks during file transfer. The function perform message validation by MAC (Message Authentication Code) and detect data errors over networks or unexpected changes of data across them.

Please use it on being enabled (performing message validation) as usual.

Related Configuration

Category	Configuration Name	Description
Server Configuration	RequireDataIntegrityChecking	Set requirement of data integrity checking by MAC
Client Common Configuration	DisableDataIntegrityChecking	Disable the data integrity checking
	AcceptDataIntegrityCheckingOnRejection	Set acceptance of rejection to disabling it

1.6.5 Transfer Resuming

This is a function to make efficient works when unexpected abortion happens on file transfer due to network problems. You can restart the transfer from the position where the previous transfer stopped if it will be aborted due to some reasons.

The hcp command of NEC Ultra-high-speed Data Transfer System provides an option of --resume (-r in short) to restart by the user operation and another one of --auto-resume to do automatically.

In the --resume option, you should specify a file to which the hcp command records its running results (saved as .hcp.out as usual) to restart it.

In the --auto-resume, the command restart the transfer when its abortion happened due to a network error. When you abort the transfer by a user operation such as Ctrl+C, restarting it will be not initiated and it will be just stopped. When you use a private key for authentication, it is recommended to use private keys without encryption. A passphrase required to decrypt the key will be cached on the memory in the process performing the transfer to avoid interactive operations for re-authentication happening after creating new connections.

And you can change a number of trials and an interval between trials for the --auto-resume option as the client configuration.

Related Option

Command	Short Name	Option Name	Description
hcp	r	resume	Resume the previous transfer
		auto-resume	Run resuming automatically (when aborted due to network problems)
		no-integrity-on-resume	Disable integrity check on resume

Related Configuration

Category	Configuration Name	Description
Client Configuration (hcp)	AutoResumeTrials	Number of auto resuming trials
	AutoResumeTrialInterval	Interval time between trials (in seconds)

1.7 Function Detail (for Supporting System Operation and Management)

1.7.1 Monitoring Functions

hcpd is available to run in foreground. All commands can output debug information (logs in debug level) if you change the level. And you can configure timeouts to detect transport disconnection or idling among operations on the server.

Please be careful of unexpected timeouts from changing the log level to debug since producing many logs makes delays of processing on file transfer on some environment, e.g. computers behind NAT.

Related Option

Command Name	Short Name	Option Name	Description
hcpd	f	fore - ground	Running in foreground
hcpd/hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		investi - gation	Running in investigation mode (deprecated)

Related Configuration

Category	Configuration Name	Description
Server Configuration	TransportTimeout	Set transport timeout
	IdleTimeout	Set idling timeout
	SystemLog	System log configuration
	SystemLogLevel	System log level
Client Common Configuration	TransportTimeout	Set transport timeout
	DiagnosticLog	Application diagnostic log configuration
	DiagnosticLogLevel	Application diagnostic log level

1.7.2 Performance Evaluation Functions

This is a function to confirm performances of data processing on sources and network communication. The function is useful for taking benchmarks on your environments and making investigation for causes from which expected performance dose not appears.

Related Option

Command Name	Short Name	Option Name	Description
hcp	N	no-send	Measure disk I/O performance in reading
hcp/hrm	n	no-diskio	Measure network I/O performance with HCP protocol

Related Configuration

Category	Configuration Name	Description
Server Configuration	MemoryTransferConcurrency	Memory copy parallelism (when disabling local disk I/O)
Client Configuration (hcp)	MemoryTransferConcurrency	Memory copy parallelism (when disabling local disk I/O)

1.7.3 Logging Management Functions

NEC Ultra-high-speed Data Transfer System provides the following types of logs.

Target	Type	Recorded Content	Initial Configuration	Default Place to Output
Server	System Log	System logs	○	/var/log/hcpd.log(Linux)
	System Statistics	traffic volume and access status on hcpd daemon running	○	/var/tmp/.hcp.statistics.system(Linux)
	Application Statistics	Run results of application	○	/var/tmp/.hcp.statistics.application(Linux)
	TCP Transport Statistics	traffic and statistics on TCP transport	-	/var/tmp/.hcp.statistics.transport.tcp.service_<service_num>.<service_port>.thread_<thread_num>(Linux)
	HpFP Transport Statistics	traffic and statistics on HpFP transport	-	/var/tmp/.hcp.statistics.transport.hpfp.service_<service_num>.<service_port>.thread_<thread_num>(Linux)
Client	File Operation Log	File operation logs	-	/var/log/hcpd.file.operation.log(Linux)
	Application Log	Application logs	○	stdout
	Application Statistics	Run results of application	○	<user_curdir>.hcp.statistics.application(Linux)
	TCP Transport Statistics	traffic and statistics on TCP transport	-	<user_curdir>.hcp.statistics.transport.tcp(Linux)
	HpFP Transport Statistics	traffic and statistics on HpFP transport	-	<user_curdir>.hcp.statistics.transport.hpfp(Linux)

* On Unix platforms, NEC Ultra-high-speed Data Transfer System also output logs from syslog subject to its system configuration.

* As other forms of recording running results, it save a running result of a command to a specific file (.hcp.out on Linux). This file is overwritten when each command runs. So the file dose not hold records before the current run.

NEC Ultra-high-speed Data Transfer System provides the following logging management functions for each type of logs.

- Destination to Output Logs

You can specify a destination to output logs by changing configuration files of a server and client or using command options.

If you use the command options, you can specify the destination each command execution. The options are 'hcp-diag' and 'stat-log-file' except for hsync. For hsync, 'hcp-diag' and 'hcp-stat-log-file' are provided as identical options for them.

- Log Level

You can set a log level to logs NEC Ultra-high-speed Data Transfer System produces. It can be chosen from EMERG, ALERT, CRIT, ERR, WARNING, INFO and DEBUG that are subject to the Severity of Syslog.

- Log Rotation

For each log, you can specify log rotation subject to threshold of a file size or date and time.

Related Option

Command Name	Short Name	Option Name	Description
hcpd	l	log-file	Set file path to save system logs
	L	stat-log-file	Set base path to save statistics
hcp/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown/hchown		hcp-diag	Set file path to save application diagnostic logs
		stat-log-file	Set base path to save statistics
		hcp-out	Set file path to save running records
		multi-run	Run in multi-running mode
hsync	v	verbose	Set verbosity of logs
		info	Set categories of logs for INFO level
	q	quiet	Set suppressing logs except for errors
		log-file	Specify a log file
		hcp-diag	Specify an application diagnostic log output destination
		hcp-stat-log-file	Specify a path of logging HCP statistics
		hcp-out	Specify a path to save HCP running records
		multi-run	Run in multi-running mode

Related Configuration

Category	Configuration Name	Description
Server Configuration	SyslogOption	Set syslog option
	SyslogFacility	Set syslog facility
	SystemLog	System log configuration
	SystemLogLevel	System log level
	ApplicationStatLog	Application statistics configuration
	TransportStatLog	Transport statistics configuration
	SystemStatLog	System statistics configuration
	FileOperationLog	File operation logging configuration
	StatLogPerUserInPrivilegeSeparation	Save statistics logs to files determined from each user (when privilege separation being enabled)
	ApplicationStatLogSecurityEx	Set to output a security detail on application statistics
Client Common Configuration	DiagnosticLog	Application diagnostic log configuration
	DiagnosticLogLevel	Application diagnostic log level
	ApplicationStatLog	Application statistics configuration
	TransportStatLog	Transport statistics configuration
	ApplicationStatLogSecurityEx	Set to output a security detail on application statistics

1.7.4 Showing Software Information

This describes functions to show information of the software itself (version), its helps and configuration status decided from configuration files and input parameters.

Normally NEC Ultra-high-speed Data Transfer System can show the information using the following options on the command line.

Related Option

Command Name	Short Name	Option Name	Description
hcpd/hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown	V	version	Display the application version
hcpd	t	config-test	Display configuration and input parameters
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		config-test	Display the configuration and input parameters
hcpd/hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown	h	help	Show command help

1.7.5 System Run-Time Configuration

For smooth operation on your system, various options, e.g. path of configuration files, PID file's specification, license key specification and signals to stop, are provided.

Related Option

Command	Short Name	Option Name	Description
hcpd	c	config-file	Set file path of configuration
	p	pid-file	Set file path to save PID
	k	license	Set file path holding license key
	q	quit	Send signal to stop
hcp/hsync/hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown		config-file	Set file path of configuration
		config-option	Make configuration from command line

- CPU Thread Limitation

This function limits a number of threads that will be running on the process of the software.

Related Configuration

Category	Configuration Name	Description
Server Configuration	MaxConcurrentThread	Limit number of threads to use (Linux)
Client Common Configuration	MaxConcurrentThread	Limit number of threads to use (Linux)

- Cooperation with External Application

This is a function to call a script (or program) when running each command of the software is finished.

Related Configuration

Category	Configuration Name	Description
Server Configuration	CallbackScript	Specify a script to call when running a command is finished

1.7.6 Manipulation of Files and Directories

You can make the following manipulation to files and directories on the server.

- Delete
- List
- Create Directory
- Print Working Directory
- Move
- Create Link
- Change File Permission
- Change Owner and Group

Related Commands

Command Name	Description
hrm	Remove files
hcp-ls	List files
hmkdir	Create directories
hpwd	Print the working directory
hmv	Move files
hln	Create links
hchmod	Change file permissions
hchown	Change owner and group of files

1.8 List of Commands Provided

NEC Ultra-high-speed Data Transfer System provides the following commands.

Command Name	Server/Client	Description	Usual Actions Corresponding to
hcpd	Server	Listening client requests to run the following client commands (for Linux)	
hcpd_session	Server	Providing privilege separation on the hcpd	
hcp	Client	File transfer	cp, scp, rsync
hsync	Client	File synchronization	rsync
hrm	Client	File deletion	ssh + rm
hcp-ls	Client	Listing files	ssh + ls/dir
hmkdir	Client	Creating directories	ssh + mkdir
hpwd	Client	Printing working directory	ssh + pwd
hmv	Client	Moving files	ssh + mv
hln	Client	Creating links	ssh + ln
hchmod	Client	Changing modes of files	ssh + chmod
hchown	Client	Changing owner and group of files	ssh + chown

1.9 Supported Platforms

The NEC Ultra-high-speed Data Transfer System will support Red Hat Enterprise Linux 9 x86_64.

1.10 Hardware Requirements

It is recommended that you use NEC Ultra-high-speed Data Transfer System on the following environments for sufficient performance to transfer files.

Server Environment

Name	Requirements
CPU	Processors corresponding to Intel Core 3GHz 4th generation or later recommended. AES-NI recommended
Memory	2GB or more (8GB recommended)
Storage	10GB free space or more (100GB recommended, but not including area for storing data files)
Network	1Gbps or more. You need network environment where HCP clients can access to the hcpd.

Client Environment (x86)

- hcp/hsync

Name	Requirements
CPU	Processors corresponding to Intel Core 3GHz 4th generation or later recommended. AES-NI recommended
Memory	1GB or more (2GB recommended)
Storage	10GB free space or more (100GB recommended, but not including area for storing data files)
Network	100Mbps or more (1Gbps recommended). If you perform a remote copy you need network environment where you can access to the hcpd.

- hrm/hcp-ls/hmkdir/hpwd/hmv/hln/hchmod/hchown

Name	Requirements
CPU	Processors corresponding to Intel Core 3GHz 4th generation or later recommended. AES-NI recommended
Memory	1GB or more (2GB recommended)
Storage	1GB free space or more (10GB recommended)
Network	100Mbps or more (1Gbps recommended). You need network environment where you can access to the hcpd.

1.11 Software Requirements

1.11.1 Dependent Libraries

On Linux, NEC Ultra-high-speed Data Transfer System depends on the following libraries.

- OpenSSL
- Zlib
- ICU
- PAM (server)

If your system does not have the above libraries installed, you need to install the libraries before installing NEC Ultra-high-speed Data Transfer System.

1.11.2 System Services

NEC Ultra-high-speed Data Transfer System manages its server software of `hcpd` by systemd On Linux. A PAM service by a system account provider is necessary to resolve user information by executing the system default authentication.

1.12 Network Requirements

In the connections over HpFP and TCP, NEC Ultra-high-speed Data Transfer System uses UDP port 65520 and TCP port 874 by default respectively. You need to make the above ports open on firewalls between a client and a server.

HpFP and TCP do not support any proxy servers.

HpFP can achieve 10 Gbps throughput with jumbo frames from 1.5 KB to 9 KB. However, less than 1.5KB frames may limit the throughput to a few Gbps, e.g., 3Gbps. Therefore, jumbo frames are essential to perform 10G throughput.

On the other hand, TCP can normally perform in more than 10Gbps environments without specific tuning. Even in LFN environments where networks are generally inefficient and slow due to many packet losses, HpFP can help enhance the performance even when jumbo frames are not available.

2 Server Setup

2.1 Red Hat Enterprise Linux (RHEL)

2.1.1 Installation of RPM Package

For the server software installation, please prepare the server latest package like the following RPM file.

* The package is not in public on the download site. Please make contact to us to get it.

```
bytix-archaea-tools-server-1.4.0-13.el9.x86_64.rpm
```

Install the package using rpm command.

```
rpm -ivh bytix-archaea-tools-server-1.4.0-13.el9.x86_64.rpm
```

If you have a license key for NEC Ultra-high-speed Data Transfer System, called as this software below, save it to the following file.

```
/etc/hcp/license.key
```

Start and stop hcpd by running the following command.

```
systemctl start hcpd  
systemctl stop hcpd
```

Edit the following files to change the server configuration and give some options to the hcpd command.

```
/etc/systemd/system/hcpd.service  
/etc/sysconfig/hcpd
```

The hcpd is installed with the following functions enabled.

- Privilege separation : Enabled
- PPAM and public key authentication : Enabled
- Cryptographic transport by a server host key : Enabled

The old package will be replaced as obsolete. Configuration files having some changes from the original one will be kept.

2.1.2 Confirm if It Works

After the installation being completed, start the server by the following command and check its status about hcpd working.

```
systemctl start hcpd  
systemctl status hcpd
```

2.1.3 Initial Configuration (around Securities)

The initial configuration is optimal in use. If you change configurations around securities, please see the configuration reference.

2.1.4 Upgrade

To upgrade on Linux, you just run the RPM command with a newer package than the current version's package using -U option.

```
rpm -Uvh bytix-archaea-tools-server-1.4.0-13.el9.x86_64.rpm
```

Old configuration files will be kept. You can make upgrade even if using a newer package in build number.

Example: Upgrade from 1.4.0-12 to 1.4.0-13

```
rpm -ivh bytix-archaea-tools-server-1.4.0-12.el9.x86_64.rpm  
rpm -Uvh bytix-archaea-tools-server-1.4.0-13.el9.x86_64.rpm (this works)
```

2.1.5 Uninstallation

To uninstall on Linux, use -e option of the RPM command to do.

```
rpm -e bytix-archaea-tools-server
```

2.2 RPM Install the software into a non-default place

When installing, please specify the following options.

```
--relocate  
--badreloc
```

And you can generate server keys on the specified place if you use the following environment variable.

```
ARCHAEA_TOOLS_INSTDIR
```

Example:

```
[user@localhost ~]$ sudo ARCHAEA_TOOLS_INSTDIR=/usr/local/archaea_tools rpm -ivh --relocate /=usr/local/archaea_tools --badreloc bytix-archaea-tools-server-1.5.0-35.el9.x86_64.rpm
```

Since the following configuration files are still supposed to be placed on /usr or /etc, please change by yourself after this installation.

```
/usr/lib/systemd/system/hcpd.service  
/etc/pam.d/hcpd  
/etc/sysconfig/hcpd
```

When uninstalling, you just make it in a normal way with specifying package names.

Do not specify --relocate and --badreloc.

Example:

```
[user@localhost ~]$ sudo ARCHAEA_TOOLS_INSTDIR=/usr/local/archaea_tools rpm -e bytix-archaea-tools-server
```

When commands are installed on non-default place, their help options (-V) shows the following information about the place.

```
[user@localhost sbin]$ ./hcpd -V  
hcp server (hcpd) 1.5.0_35 / Linux (HpFP2 2.0.0.91_21 WSAPI 0.0.1.30 WS 4.2.0-1)  
Installed prefix: /usr/local/archaea_tools (/usr/local/archaea_tools/usr/sbin/hcpd)
```

2.3 RPM Install the software by non-privileged users

When installing, please specify the following options.

```
--relocate  
--badreloc  
--nodeps  
--dbpath
```

Installation registry information will be saved at the place specified by the `--dbpath` option that is a directory where you want to save the information.

And you can skip unnecessary processing, e.g. systemd service registration, for non-privileged users if you use the following environment variable.

```
ARCHAEA_TOOLS_USER_INSTALL yes
```

Example:

```
[user@localhost ~]$ export ARCHAEA_TOOLS_USER_INSTALL=yes
[user@localhost ~]$ export ARCHAEA_TOOLS_INSTDIR=/home/user/archaea_tools
[user@localhost ~]$ rpm -ivh --nodeps --dbpath=/home/user/rpm --relocate /=/home/user/archaea_tools --badreloc bytix-archaea-tools-server-1.5.0-35.el9.x86_64.rpm
```

Please make the following attentions when using the server package in the above manner.

- No to use systemd. Run the `hcpd` command by yourself.
- Use non-privileged port numbers.
- Specify PID file from command line.
- When you cannot access to PAM authentication and account information by non-privileged users, please consider to use UID/GID specification and public usage (anonymous access with port number limitation or network access limitation).

When uninstalling, please specify the following options.

```
--nodeps
--dbpath
```

* Do not specify `--relocate` and `--badreloc`.

Example:

```
[user@localhost ~]$ rpm -e --nodeps --dbpath=/home/user/rpm bytix-archaea-tools-server
```

For servers, you need the following packages on your system.

```
libc, pam, openssl, zlib
```

You can confirm them by `--qa` option of the `rpm` command.

Example:

```
[user@localhost ~]$ rpm -qa | grep -E -e "^(libc|pam|openssl|zlib)-"
libc-67.1-9.el9.x86_64
openssl-pkcs11-0.4.11-7.el9.x86_64
libc-devel-67.1-9.el9.x86_64
openssl-libs-3.0.1-43.el9_0.x86_64
openssl-devel-3.0.1-43.el9_0.x86_64
openssl-3.0.1-43.el9_0.x86_64
pam-1.5.1-12.el9.x86_64
pam-devel-1.5.1-12.el9.x86_64
zlib-1.2.11-35.el9_1.x86_64
zlib-devel-1.2.11-35.el9_1.x86_64

[user@localhost ~]$ find /usr/lib64 | grep -E -e "^/usr/lib64/lib(icudata|icuuc|pam|crypto|ssl|z)¥."
/usr/lib64/libicudata.so.67.1
/usr/lib64/libicudata.so.67
/usr/lib64/libz.so.1
/usr/lib64/libz.so.1.2.11
/usr/lib64/libicuuc.so.67
/usr/lib64/libicuuc.so.67.1
/usr/lib64/libcrypto.so.3
/usr/lib64/libcrypto.so.3.0.1
/usr/lib64/libssl.so.3
/usr/lib64/libssl.so.3.0.1
/usr/lib64/libpam.so.0.85.1
/usr/lib64/libpam.so.0
/usr/lib64/libcrypto.so
/usr/lib64/libz.so
/usr/lib64/libssl.so
/usr/lib64/libicudata.so
/usr/lib64/libicuuc.so
/usr/lib64/libpam.so
```

2.4 How to use hcpd by users without privilege

Save hcpd configuration files under your home directory at the following paths.

```
~/hcpd.conf
~/ .hcp/hcpd.conf
```

Change the service ports to port numbers that do not require privilege.

```
TCPListenAddress 0.0.0.0:1874
HPFPListenAddress 0.0.0.0
* Edit hcpd.conf.
```

If you use a license key, save it under your home directory at the following paths.

```
~/hcp_license.key
~/.hcp/license.key
```

Start hcpd daemon by running hcpd command and specifying a configuration file, a PID file, and a license key as command options.

```
hcpd -c ~/hcpd.conf -p ~/hcpd.pid -k ~/hcp_license.key
```

Please be careful of collision of PID files or port numbers of transport services like TCP if hcpd daemon is running.

3 Server Command

3.1 Server Command (hcpd)

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.

3.1.1 Basic Format

The basic format is as follows.

```
Usage: hcpd [OPTION] ...  
or : hcpd -q [OPTION] ...  
or : hcpd --auth-keys [OPTION] ... [PATH]
```

3.1.2 Option List

The options for the hcpd commands are below.

Various Monitorings

Description	Short Name	Option Name
Foreground execution	f	<u>foreground</u>
Investigation mode starts (deprecated)		<u>investigation</u>

Log Management

Description	Short Name	Option Name
Specify a system log output destination	l	<u>log-file</u>
Specify various statistics log output destinations	L	<u>stat-log-file</u>

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters	t	<u>config-test</u>
Display the hcpd daemon help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting a path of the configuration file	c	<u>config-file</u>
Setting a file path to save a process ID	p	<u>pid-file</u>
Setting a file path to save a license key	k	<u>license</u>
The stop command	q	<u>quit</u>

Check System Information

Description	Short Name	Option Name
Show system info		<u>system-info</u>
Run host benchmark		<u>run-host-benchmark</u>
Specify measurement categories on the benchmark		<u>run-host-benchmark-categories</u>

Fetching User's Public Keys

Description	Short Name	Option Name
Fetch authorized_keys		<u>auth-keys</u>
Specify UID on fetching it		<u>auth-keys-uid</u>
Specify user name on fetching it		<u>auth-keys-user</u>
Specify ability of system auth (PAM) on fetching it		<u>auth-keys-sys-auth-disabled</u>
Disable supplemental groups on fetching it		<u>auth-keys-no-supp-groups</u>

3.1.3 Various Monitorings

3.1.3.1 f, foreground

```
=====
Format : -f | --foreground
=====
```

Start the hcpd daemon in the foreground mode.

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

3.1.3.2 investigation

```
=====
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.

This option is deprecated. Instead, detailed log data can be obtained with SystemLogLevel or DiagnosticLogLevel DEBUG.

3.1.4 Log Management

3.1.4.1 l, log-file

```
=====
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.

3.1.4.2 L, stat-log-file

```
=====
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>.thread_<thre
ad number>.transport.tcp (TCPtransport statistics)
<spciified path>.transport.hpfp.service_<service number>.<t;service port>.thread_<t
hread number>(HpFPtransport 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)
```

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

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

3.1.5 Software Information Update

3.1.5.1 V, version

```
=====
Format : -V | --version
=====
```

Display the hcpd daemon version.

```
--
Example:
[root@localhost ~]# hcpd -V
hcp server (hcpd) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

3.1.5.2 t, config-test

```
=====
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
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/authorized_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          : 1143472128 [auto=yes, mode=session]
MaxBufferSize               : 104857600
MaxTotalReceiveRate          : 100000000000
MaxTotalSendRate             : 100000000000
MaxReceiveRate               : 100000000000

```

```

MaxSendRate                : 100000000000
MaxConnectionReceiveRate   : 100000000000
MaxConnectionSendRate      : 100000000000
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=104857600, rcvb
uf=209715200, mss=-1, mcd=1]
ListenServiceBonding       : -
UDPServiceExtensionBufferSize : 762314752 [auto=yes]
TCPServiceSocketSendBuffer : 0
AcceptableCryptMethod      : AES256/GCM AES256/CTR/VMAC AES256/CBC AES128/CB
C [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, pattern=no:] -[/
var/log/hcpd.log]
ApplicationStatLog          : yes Rotation[size=no:0:0, pattern=no:]
TransportStatLog            : no Rotation[size=no:0:0, pattern=no:]
SystemStatLog               : yes Rotation[size=no:0:0, pattern=no:]
FileOperationLog            : no -[/var/log/hcpd.file.operation.log] Rotation
[size=no:0:0, pattern=no:]
CallbackScript              : no Script[~/ .hcp/callback.sh, data=~/ .hcp/callb

```

```

ack]
CallbackScriptHomeIsolation      : no [logical=no]
CallbackScriptNoSymbolicLink     : no
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 4MB 8MB 16MB
24MB 32MB
GetGrRMaxBufferSize              : 524288
GetPwRMaxBufferSize              : 65536
-----

```

3.1.5.3 h, help

```

=====
Format : -h | --help
=====

```

Display the hcpd daemon help.

```

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

```

3.1.6 System Operating Environment Settings

3.1.6.1 c, config-file

```
=====
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. It is executed when normal users use the hcpd commands or when individual settings are necessary for each user.

```
--
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
```

3.1.6.2 p, pid-file

```
=====
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.

3.1.6.3 k, license

```
=====
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
Max multiple connection degree per session 1
```

3.1.6.4 q, quit

```
=====
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 ...  
--
```

3.1.7 Check System Information

3.1.7.1 system-info

```
=====  
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 ... --

3.1.7.2 run-host-benchmark

```
=====  
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 ... --

3.1.7.3 run-host-benchmark-categories

```
=====
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 ...
--
```

3.1.8 Fetching User's Public Keys

3.1.8.1 auth-keys

```
=====
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" // fetch only fro
m the .hcp directory. suppress tilde expansion
--
```

3.1.8.2 auth-keys-uid

```
=====
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 ...
--
```

3.1.8.3 auth-keys-user

```
=====
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 ...
--
```

3.1.8.4 auth-keys-sys-auth-disabled

```
=====
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 ...  
--
```

3.1.8.5 auth-keys-no-supp-groups

```
=====  
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 ...  
--
```

4 Server Configuration

4.1 Server Setting Files

NEC Ultra-high-speed Data Transfer System provides the following configuration files on the server.

File Name	File Path in Default	Important Configurations
System configuration files of hcpd (or hcpd_winserv) daemon	/etc/hcp/hcpd.conf	transport services (TCP/HpFP), server security, authentication, logging, statistics and tuning parameters
Service description file for systemd daemon	/usr/lib/systemd/system/hcpd.service	
PAM authentication configuration file	/etc/pam.d/hcpd	

4.2 Server Setting Items

4.2.1 Setting Item List

The setting items for the hcpd daemon are below.

System Operating Environment Settings, Transmission Method Related

Description	Configuration Name
Protocol version (fixed to 2)	ProtocolVersion
TCP service listen address setting	<u>TCPListenAddress</u>
HpFP service listen address	<u>HPFPListenAddress</u>
HpFP service listen address (bi-port type, deprecated)	<u>UDPListenAddress</u>
Listen service bonding	<u>ListenServiceBonding</u>

Communication Data Compression Function

Description	Configuration Name
Header compression (reserved)	<u>HeaderCompress</u>
Content compression (reserved)	<u>ContentCompress</u>

Data Flow Control, Bandwidth Control

Description	Configuration Name
Maximum total receiving rate (entire system)	<u>MaxTotalReceiveRate</u>
Maximum total sending rate (entire system)	<u>MaxTotalSendRate</u>
Maximum receiving rate (per session)	<u>MaxReceiveRate</u>
Maximum sending rate (per session)	<u>MaxSendRate</u>
Maximum receiving rate (per connection)	<u>MaxConnectionReceiveRate</u>
Maximum sending rate (per connection)	<u>MaxConnectionSendRate</u>

Data Flow Control, File Lock Function

Description	Configuration Name
Use file lock	<u>FileLock</u>
Number of trials to lock files	<u>FileLockTrials</u>
The trial interval (in seconds)	<u>FileLockTrialInterval</u>

Data Flow Control, Temporary File Save Function (Atomic File Save)

Description	Configuration Name
Atomically file saving	<u>AtomicLikeSaving</u>
Threshold for atomically file saving	<u>AtomicLikeSavingThreshold</u>
Reject requests to overwriting temporary files which already exist when atomically file saving	<u>AtomicLikeSavingRejectOverwriteRequest</u>

Data Flow Control, Data Buffer Setting

Description	Configuration Name
Maximum buffer allocation size (entire system)	<u>MaxTotalBufferSize</u>
Maximum buffer allocation size (per connection)	<u>MaxBufferSizePerConnection</u>
TCP sending buffer	<u>TCPServiceSocketSendBuffer</u>
HpFP service extension buffer size	<u>UDPServiceExtensionBufferSize</u>
HpFP service protected shared memory	<u>HPFPProtectedSharedMemory</u>
Max buffer size for getgrxxx_r functions	<u>GetGrRMaxBufferSize</u>
Max buffer size for getpwxxx_r functions	<u>GetPwRMaxBufferSize</u>

Data Flow Control, Transfer File Size Control

Description	Configuration Name
Maximum receiving file size	<u>MaxReceiveFileSize</u>
Maximum sending file size	<u>MaxSendFileSize</u>

Data Flow Control, Message Data Size Control

Description	Configuration Name
Initial header block size	<u>InitHeaderBlockSize</u>
Initial content block size	<u>InitContentBlockSize</u>
Maximum header block size	<u>MaxHeaderBlockSize</u>
Maximum content block size	<u>MaxContentBlockSize</u>
Max file entry request	<u>MaxRequestFileEntryAtOnce</u>

Data Flow Control, Disk I/O Speed Control

Description	Configuration Name
Disk I/O reading rate per session	<u>MaxReadRate</u>
Disk I/O writing rate per session	<u>MaxWriteRate</u>

Code Transformation, Communication Encoding Negotiation

Description	Configuration Name
Transport character encoding	<u>TransportCharEncoding</u>

Code Transformation, Host Character Encoding

Description	Configuration Name
Host character encoding	<u>HostEncoding</u>

Authentication

Description	Configuration Name
PAM (Pluggable Authentication Module) authentication	<u>PAMAuthentication</u>
Public key authentication	<u>PubkeyAuthentication</u>
Maximum number of authentication tries	<u>MaxAuthTries</u>
Specify directory for searching public keys (RSA auth)	<u>AuthorizedKeysSearchDir</u>
Specify file for finding a public key (RSA auth)	<u>AuthorizedKeysFile</u>
Specify command for finding a public key (RSA auth)	<u>AuthorizedKeysCommand</u>
Specify user to run the command (RSA auth)	<u>AuthorizedKeysCommandUser</u>
Specify user name pattern to allow login	<u>AllowUsers</u>
Specify group name pattern to allow login	<u>AllowGroups</u>
Specify user name pattern to deny login	<u>DenyUsers</u>
Specify group name pattern to deny login	<u>DenyGroups</u>

Encryption

Description	Configuration Name
Encryption method for message communication	<u>AcceptableCryptMethod</u>
Digest method for validation of message and file data	<u>AcceptableDigestMethod</u>
Setting requirement of MAC (Message Authentication Code)	<u>RequireDataIntegrityChecking</u>

Security Negotiation by Encryption Communications

Description	Configuration Name
Server key path for the server authentication	<u>ServerKeyFile</u>

Access Control

Description	Configuration Name
Fallback control from user home (for backward compatibility)	<u>UserDirectoryFallbackAvailable</u>
Access rejection when a directory of user home is not found	<u>RejectOnUserHomeDirectoryNotFound</u>

Access Control, Privilege Separation

Description	Configuration Name
Set privilege separation	<u>UsePrivilegeSeparation</u>
Minimum UID applicable for privilege separated sessions	<u>PrivilegeSeparationMinimumUID</u>
Minimum GID applicable for privilege separated sessions	<u>PrivilegeSeparationMinimumGID</u>
Default user on privilege separation (applied when any user is not determined)	<u>PrivilegeSeparationUser</u>
Umask on privilege separation for authenticated users	<u>PrivilegeSeparationUmask</u>
Umask on privilege separation for anonymous	<u>PrivilegeSeparationUmaskAnonymous</u>
Apply user's access rights to file permissions on destination (not on privilege separation)	<u>ApplyUserPermission</u>
Disable supplemental groups	<u>NoSupplementalGroupInPrivilegeSeparation</u>

Access Control, ACL (Access Control List) Function

Description	Configuration Name
Define ACL (Access Control List)	<u>AccessList</u>
Define Allow rules on ACL	<u>Allow</u>
Define Deny rules on ACL	<u>Deny</u>

Access Control, Admission Control

Description	Configuration Name
Limit of connections (total)	<u>MaxTotalConnection</u>
Limit of TCP connections	<u>MaxTcpConnection</u>
Limit of UDP (HpFP) connections	<u>MaxUdpConnection</u>
Limit of connections each user	<u>MaxConnectionPerUser</u>
Limit of connections to accept each second	<u>MaxConnectionPerSec</u>

Access Control, Document Point

Description	Configuration Name
Define a document point	<u>DocPoint</u>
Specify a path on file system on the document point	<u>DocPath</u>
Set user home isolation	<u>HomeIsolation</u>
Set reading access configuration	<u>PermitAccessRead</u>
Set writing access configuration	<u>PermitAccessWrite</u>
Set overwriting access configuration	<u>PermitAccessOverwrite</u>
Set deleting access configuration	<u>PermitAccessDelete</u>
Set reading in random access configuration (Reserved)	<u>PermitAccessRandomRead</u>
Set writing in random access configuration (Reserved)	<u>PermitAccessRandomWrite</u>

Various Monitoring, Timeout Control

Description	Configuration Name
Set transport timeout	<u>TransportTimeout</u>
Set idling timeout	<u>IdleTimeout</u>

Performance Evaluation

Description	Configuration Name
How to make pre-allocation in disk benchmark	<u>DiskBenchmarkPreAllocation</u>
A unit size for the pre-allocation	<u>DiskBenchmarkPreAllocationSize</u>
Direct I/O benchmark, alignment size specification	<u>DiskBenchmarkDirectAlignmentSize</u>
Async I/O benchmark, NO_WAIT(reserved)	<u>DiskBenchmarkAsyncNoWait</u>
Async I/O benchmark, maximum number of I/O events at once	<u>DiskBenchmarkAsyncMaxEvents</u>
Async I/O benchmark, maximum number of taking event results at once	<u>DiskBenchmarkAsyncMaxGetEvents</u>
Async I/O benchmark, a size of pool holding request buffers	<u>DiskBenchmarkAsyncRequestPoolSize</u>
File size on additional disk benchmarks	<u>DeepDiskBenchmarkFileSize</u>
Required free space on the benchmarks	<u>DeepDiskBenchmarkFreeSpaceRequired</u>
A set of block sizes on the benchmarks	<u>DeepDiskBenchmarkBlockSizes</u>
Memory copy parallelism (when disabling local disk I/O)	<u>MemoryTransferConcurrency</u>

Log Management

Description	Configuration Name
Set syslog option	<u>SyslogOption</u>
Set syslog facility	<u>SyslogFacility</u>
System log configuration	<u>SystemLog</u>
System log level	<u>SystemLogLevel</u>
Application statistics configuration	<u>ApplicationStatLog</u>
Transport statistics configuration	<u>TransportStatLog</u>
System statistics configuration	<u>SystemStatLog</u>
File operation logging configuration	<u>FileOperationLog</u>
Save statistics logs to files determined from each user (when privilege separation being enabled)	<u>StatLogPerUserInPrivilegeSeparation</u>
Set to output a security detail on application statistics	<u>ApplicationStatLogSecurityEx</u>

System Operating Environment Settings, CPU Thread Control

Description	Configuration Name
Limit number of threads to use (Linux)	<u>MaxConcurrentThread</u>

System Operating Environment Settings, Application Linked Function

Description	Configuration Name
Specify a script to call when running a command is finished	<u>CallbackScript</u>
Call back script home isolation	<u>CallbackScriptHomeIsolation</u>
Call back script ignores symbolic links	<u>CallbackScriptNoSymbolicLink</u>

Others

Description	Configuration Name
Ensure to transfer files to the destination directory (for backward compatibility)	<u>EnsureDestinationInFileTransfer</u>

4.2.2 System Operating Environment Settings, Transmission Method Related

4.2.2.1 TCPListenAddress

```
=====
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 an optional setting. It 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  
--
```

4.2.2.2 HPFPListenAddress

```
=====  
Format : HPFPListenAddress <hfpf_service_addr>[:<hfpf_service_port>[:<hfpf_sndbuf>[:  
:<hfpf_rcvbuf>[:<hfpf_mss>[:<mcd>]]]]][ <acl_name>]  
-----  
hfpf_service_addr  
Default : none  
Range of Values : IP address  
-----  
hfpf_service_port  
Format : <decimal_number>  
Default : 65520  
Range of Values : decimal_number is 1-65535.  
-----  
hfpf_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.  
-----  
hfpf_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.  
-----  
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's + 1, logical-CPU's/2 + 1, 25 or 1  
Range of Values : 1 - 65535  
-----  
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.

hfp_service_addr specifies the IP address for HpFP service.

hfp_service_port is the port number of UDP transport for HpFP protocol in the optional setting.

hfp_sndbuf is the transmission buffer size in the optional setting. “D” stands for default.

hfp_rcvbuf is the buffer size for received data by HpFP protocol in the optional setting. “D” stands for default.

hfp_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)

acl_name is an optional setting, as in TCP service. It is a name of an access control list (see AccessList) that you would like to set to the HpFP 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 HpFP service.

```
--
Example :
HPFPListenAddress 0.0.0.0:10000
--
```

4.2.2.3 UDPListenAddress

```
=====
Format : UDPListenAddress <hfp_service_addr>[:<hfp_service_port>[:<hfp_udp_port>
[:<hfp_sndbuf>[:<hfp_rcvbuf>[:<hfp_mss>[:<mcd>]]]]][ <acl_name>]
-----
hfp_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 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 )
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.

hpfp_service_addr specifies the IP address for HpFP service.

hpfp_service_port is a port number of the HpFP service in the optional setting.

hpfp_udp_port is the port number of UDP transport for HpFP protocol in the optional setting. “D” stands for default.

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)

acl_name is an optional setting, as in TCP service. It is a name of an access control list (see AccessList) that you would like to set to the HpFP(UDP) 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 HpFP(UDP) service.

```
--  
Example :  
UDPListenAddress 0.0.0.0:1884:10000  
--
```

4.2.2.4 ListenServiceBonding

```
=====  
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  
--
```

4.2.3 Communication Data Compression Function

4.2.3.1 HeaderCompress (reserved)

4.2.3.2 ContentCompress (reserved)

4.2.4 Data Flow Control, Bandwidth Control

4.2.4.1 MaxTotalReceiveRate

```
=====  
Format : MaxTotalReceiveRate <bandwidth>  
-----  
bandwidth  
Default : 100Gbit  
Range of Values : unsigned double-length integer  
=====
```

The traffic shaping control on the receiving bandwidth for the transport is configured (entire system). This function realizes the bandwidth control between the TCP/HpFP (UDP) layer and the application layer.

```
--  
Example :  
MaxTotalReceiveRate 1Gbit  
--
```

This function realizes the bandwidth control between the TCP/HpFP (UDP)/ 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.

4.2.4.2 MaxTotalSendRate

```
=====
Format : MaxTotalSendRate <bandwidth>
-----
bandwidth
Default : 100Gbit
Range of Values : unsigned double-length integer
=====
```

The traffic shaping control on the sending bandwidth for the transport is configured (entire system). This function realizes the bandwidth control between the TCP/HpFP (UDP) layer and the application layer.

```
--
Example :
MaxTotalSendRate 1Gbit
--
```

4.2.4.3 MaxReceiveRate

```
=====
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
--
```

4.2.4.4 MaxSendRate

```
=====
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
--
```

4.2.4.5 MaxConnectionReceiveRate

```
=====
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 session is configured (per connection). This function realizes the bandwidth control between the TCP/HPFP (UDP) layer and the application layer.

```
--
Example :
MaxConnectionReceiveRate 100Mbit
--
```

The old name of 'MaxReceiveRatePerConnection' is available.

4.2.4.6 MaxConnectionSendRate

```
=====
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 session is configured (per connection). This function realizes the bandwidth control between the TCP/HpFP (UDP) layer and the application layer.

```
--
Example :
MaxConnectionSendRate 100Mbit
--
```

The old name of 'MaxSendRatePerConnection' is available.

4.2.5 Data Flow Control, File Lock Function

4.2.5.1 FileLock

```
=====
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 net - work filesystems like NFS or some errors occurs on acquiring file locks. Please be careful of conflicts on destina - tions 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 was rejected at the first trial.
2018/07/05 16:34:13 00007f638bd97740:INFO :Acquiring a lock to the file continues 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
--
```

4.2.5.2 FileLockTrials

```
=====
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.

4.2.5.3 FileLockTrialInterval

```
=====
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.

4.2.6 Data Flow Control, Temporary File Save Function (Atomic File Save)

4.2.6.1 AtomicLikeSaving

```
=====
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 prefix 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. The default length of the random string is 6.

4.2.6.2 AtomicLikeSavingThreshold

```
=====
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.

4.2.6.3 AtomicLikeSavingRejectOverwriteRequest

```
=====
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.

4.2.7 Data Flow Control, Data Buffer Setting

4.2.7.1 MaxTotalBufferSize

```
=====
Format : MaxTotalBufferSize <max-total-buf-size>[ <mode>]
-----
max-total-buf-size
Default : 4GB or auto calculated
Range of Values : signed double-length integer, auto
-----
mode
Default : session
Range of Values : session, operation (Linux.x86)
=====
```

The maximum memory buffer size for file data processing on the hcpd daemon and a method to make the limitation is configured.

max-total-buf-size determines a maximum buffer size for file data processing on the hcpd daemon. If this option is not specified, that size will be determined as 40% (30% if HpFP is on) of the size of the system memory or 4GB (when cannot detect the size).

mode specifies a method to make limitation of consuming the buffer. If you specify 'session', each session can use an amount of memory for that processing in a size obtained by equally dividing max-total-buf-size by a number of user sessions. If you specify 'operation', each session can use another amount of memory for that processing in a size obtained by equally dividing max-total-buf-size by a number of user sessions that are actually performing file transfers. You do not need 'operation' when all clients only use hcp command or hsync command. However, it will improve memory usage efficiency since user sessions that do not make file transfers are not in count. 'operation' is available only for Linux environment with privilege separation.

DisableMemoryManager was removed. Please set this max-total-buf-size to -1 instead when you want to disable the limitation as if specifying DisableMemoryManager = yes in the previous version.

```
--
Example :
MaxTotalBufferSize 8GB
MaxTotalBufferSize auto operation
--
```

4.2.7.2 MaxBufferSize

```
=====
Format : MaxBufferSize <max-buf-size>
-----
max-buf-size
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 :
MaxBufferSize 512MB
--
```

The old name of 'MaxBufferSizePerConnection' is available.

4.2.7.3 TCPServiceSocketSendBuffer

```
=====
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
--
```

4.2.7.4 UDPServiceExtensionBufferSize

```
=====
Format : UDPServiceExtensionBufferSize <ext-buf-size>
-----
ext-buf-size
Default : 2GB or auto calculated (Linux.x86)
Range of Values : unsigned double-length integer (byte), auto (Linux.x86)
=====
```

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 (`hpfp_sndbuf` or `hpfp_rcvbuf` 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. If this option is not specified, that size will be determined as 20% of the size of the system memory or 2GB (when cannot detect the size).

When “0”, this extension doesn’t work.

The initial buffer size (the buffer size before extended) is 1MB.

```
--
Example :
UDPServiceExtensionBufferSize 4GB
--
```

4.2.7.5 HPFPProtectedSharedMemory

```
=====
書式 : HPFPProtectedSharedMemory <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

When the privilege separation is available, this option enables a protected mode of a shared memory used by the HpFP(UDP) service.

This option is in release candidate. It might be modified because, in sometime, high latency can occur when session negotiation is aborted.

```
--
Example :
HPFPProtectedSharedMemory no
--
```

4.2.7.6 GetGrRMaxBufferSize

```
=====
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
--
```

4.2.7.7 GetPwRMaxBufferSize

```
=====
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
--
```

4.2.8 Data Flow Control, Transfer File Size Control

4.2.8.1 MaxReceiveFileSize

```
=====
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
--
```

4.2.8.2 MaxSendFileSize

```
=====
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
--
```

4.2.9 Data Flow Control, Message Data Size Control

4.2.9.1 InitHeaderBlockSize

```
=====
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.

4.2.9.2 InitContentBlockSize

```
=====
Format : InitContentBlockSize <block-size>
-----
block-size
Default : 1MB
Range of Values : unsigned double-length integer
=====
```

The initial content block size is configured.

In environments over 10Gbps, when the communication performance hits a peak by making the most of it, changing InitContentBlockSize along with MaxContentBlockSize may reach an even better performance.

```
--
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.

4.2.9.3 MaxHeaderBlockSize

```
=====
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.

4.2.9.4 MaxContentBlockSize

```
=====
Format : MaxContentBlockSize <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 MaxContentBlockSize along with InitContentBlockSize may reach an even better performance.

```
--
Example :
MaxContentBlockSize 4MB
--
```

Once the transmission starts, the occupied bandwidth is measured and the content block size is changed into the available size.

4.2.9.5 MaxRequestFileEntryAtOnce

```
=====
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
--
```

4.2.10 Data Flow Control, Disk I/O Speed Control

4.2.10.1 MaxReadRate

```
=====
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.

4.2.10.2 MaxWriteRate

```
=====  
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.

4.2.11 Code Transformation, Communication Encoding Negotiation

4.2.11.1 TransportCharEncoding

```
=====  
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.

4.2.12 Code Transformation, Host Character Encoding

4.2.12.1 HostEncoding

```

=====
Format : HostEncoding <encoding>
-----
encoding
Default :
    UTF-8 (Linux)
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.

4.2.13 Authentication

4.2.13.1 PAMAuthentication

```
=====
Format : PAMAuthentication <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

PAM(Pluggable Authentication Module) 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
```

4.2.13.2 PubkeyAuthentication

```
=====
Format : PubkeyAuthentication <flag-available>
-----
flag-available
Default : yes (Linux.x86)
Range of Values : yes, no
=====
```

Public key authentication is specified. It is enabled by inputting “yes”.

```
--
Example :
PubkeyAuthentication no
--
```

4.2.13.3 MaxAuthTries

```
=====
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
--
```

4.2.13.4 AuthorizedKeysSearchDir

```
=====
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.

4.2.13.5 AuthorizedKeysFile

```
=====
Format : AuthorizedKeysFile <file-path>
-----
file-path
Default :
  ~/.hcp/authorized_keys (Linux.x86)
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 %, %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.

4.2.13.6 AuthorizedKeysCommand

```
=====
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 user - name 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 %, %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
```

4.2.13.7 AuthorizedKeysCommandUser

```
=====
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
```

4.2.13.8 AllowUsers

```
=====  
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 --

4.2.13.9 AllowGroups

```
=====
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 --

4.2.13.10 DenyUsers

```
=====
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 --

4.2.13.11 DenyGroups

```
=====
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 --

4.2.14 Encryption

4.2.14.1 AcceptableCryptMethod

```
=====
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/HMAC,
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.

4.2.14.2 AcceptableDigestMethod

```
=====
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 for data communication and verification of transferred files 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.

4.2.14.3 RequireDataIntegrityChecking

```
=====
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
--
```

4.2.15 Security Negotiation by Encryption Communications

4.2.15.1 ServerKeyFile

```
=====
Format : ServerKeyFile <file-path>[ <serv-key-name>]
-----
file-path
Default :
    /etc/hcp/key/server.key (Linux.x86)
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”, server authentication is performed by using this pair of keys.

server-key-name is optional.

```
--
Example :
ServerKeyFile /etc/hcp/key/server.key
ServerKeyFile /etc/hcp/key/server.wss.key wss-key
--
```

When client users access to 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+FQ9577NIRYxRquZ6eWA=.
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>/ .hcp/known_hosts (Linux)
```

4.2.16 Access Control

4.2.16.1 UserDirectoryFallbackAvailable

```
=====
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
--
```

4.2.16.2 RejectOnUserHomeDirectoryNotFound

```
=====
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
--
```

4.2.17 Access Control, Privilege Separation

4.2.17.1 UsePrivilegeSeparation

```
=====
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.

```
--
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.

4.2.17.2 PrivilegeSeparationMinimumUID

```
=====
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 --

4.2.17.3 PrivilegeSeparationMinimumGID

```
=====
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 --

4.2.17.4 PrivilegeSeparationUser

```
=====
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  
--
```

4.2.17.5 PrivilegeSeparationUmask

```
=====  
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).

```
--  
Example :  
PrivilegeSeparationUmask 0002  
--
```

4.2.17.6 PrivilegeSeparationUmaskAnonymous

```
=====
Format : PrivilegeSeparationUmaskAnonymous <umask_val>[ <dir_umask_val>]
-----
umask_val
Default : 0002
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
--
```

4.2.17.7 ApplyUserPermission

```
=====
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  
--
```

4.2.17.8 NoSupplementalGroupInPrivilegeSeparation

```
=====  
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  
--
```

4.2.18 Access Control, ACL (Access Control List) Function

4.2.18.1 AccessList

```
=====  
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.

4.2.18.2 Allow

```
=====
Format : Allow (<ip_addr> <net_mask>|any) [ <hpfp_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)[...]
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.

4.2.18.3 Deny

```
=====
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.

4.2.19 Access Control, Admission Control

4.2.19.1 MaxTotalConnection

```
=====
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
--

```

4.2.19.2 MaxTcpConnection

```

=====
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
--

```

4.2.19.3 MaxUdpConnection

```

=====
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
--
```

4.2.19.4 MaxConnectionPerUser

```
=====
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
--
```

4.2.19.5 MaxConnectionPerSec

```
=====
Format : MaxConnectionPerSec <max-con-per-sec>
-----
max-con-per-sec
Default : 50
Range of Values : signed integer
=====
```

The maximum number of connections per second is configured.

```
--
Example :
MaxConnectionPerSec 10
--
```

4.2.20 Access Control, Document Point

4.2.20.1 DocPoint

```
=====
Format : DocPoint <doc_point_name>
-----
doc_point_name
Default : none
Range of Values : characters
=====
```

This option specifies an area on the file system of the server to provide available accesses to clients under a directory and its children. It includes some configurations to set write and read permission.

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
    DocPath /home
    PermitAccessRead yes
    PermitAccessWrite yes
    PermitAccessOverwrite yes
    PermitAccessDelete yes
DocPointEnd
--
```

[DocPath](#), [PermitAccessRead](#), [PermitAccessWrite](#), [PermitAccessOverwrite](#), [PermitAccessDelete](#)

When you configure two or more DocPoints, list the descriptions like the following example.

```
--
Example :
DocPoint /home
    .....
DocPointEnd

DocPoint /dev
```

```
.....
DocPointEnd
--
```

4.2.20.2 DocPath

```
=====
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.

4.2.20.3 HomeIsolation

```
=====
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.

4.2.20.4 PermitAccessRead

```
=====
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.

4.2.20.5 PermitAccessWrite

```
=====
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.

4.2.20.6 PermitAccessOverwrite

```
=====
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.

4.2.20.7 PermitAccessDelete

```
=====
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.

4.2.20.8 PermitAccessRandomRead (reserved)

```
=====  
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  
--
```

4.2.20.9 PermitAccessRandomWrite (reserved)

```
=====  
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  
--
```

4.2.21 Various Monitoring, Timeout Control

4.2.21.1 TransportTimeout

```
=====
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
--
```

4.2.21.2 IdleTimeout

```
=====
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 Archaea dialog.

0 indicates disabling the timeout.

```
--
Example :
IdleTimeout 180
--
```

4.2.22 Performance Evaluation

4.2.22.1 DiskBenchmarkPreAllocation

```
=====
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
--
```

4.2.22.2 DiskBenchmarkPreAllocationSize

```
=====
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 benchmark (one time allocation).

```
--
Example :
DiskBenchmarkPreAllocationSize 1GB
--
```

4.2.22.3 DiskBenchmarkDirectAlignmentSize

```
=====
Format : DiskBenchmarkDirectAlignmentSize <alignment-size>
-----
alignment-size
Default : 0
Range of Values : unsigned double-length integer
=====
```

This option specifies 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
--
```

4.2.22.4 DiskBenchmarkAsyncNoWait (Reserved)

4.2.22.5 DiskBenchmarkAsyncMaxEvents

```
=====
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
--

```

4.2.22.6 DiskBenchmarkAsyncMaxGetEvents

```

=====
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
--

```

4.2.22.7 DiskBenchmarkAsyncRequestPoolSize

```
=====
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
--
```

4.2.22.8 DeepDiskBenchmarkFileSize

```
=====
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
--
```

4.2.22.9 DeepDiskBenchmarkFreeSpaceRequired

```
=====
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
--
```

4.2.22.10 DeepDiskBenchmarkBlockSizes

```
=====
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
--
```

4.2.22.11 MemoryTransferConcurrency

```
=====
Format : MemoryTransferConcurrency <num-concur> <wait-type> <busy-sleep-nsec>
-----
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 se
conds
--
```

4.2.23 Log Management

4.2.23.1 SyslogOption

```
=====
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
--
```

4.2.23.2 SyslogFacility

```
=====
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
--
```

4.2.23.3 SystemLog

```
=====
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 00:05 (In re  
starting, 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  
--
```

4.2.23.4 SystemLogLevel

```
=====
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
--
```

4.2.23.5 ApplicationStatLog

```
=====
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 “DatePatterns” 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
--
```

4.2.23.6 TransportStatLog

```
=====
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 “DatePatterns” 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>

```

```
d_<thread number>.2019-12-10
<specified path>.transport.tcp.service_<service number>.<service port number>.threa
d_<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
--
```

4.2.23.7 SystemStatLog

```
=====
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 “DatePatterns” 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
--
```

4.2.23.8 FileOperationLog

```
=====
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 “DatePatterns” 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)
```

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-operat
ion-label>] <path>...
yyyy/mm/dd HH:MM:SS.<usec> <remote-ip> <username> <file-io-operation-name>\[<hcp-op
eration-name>\] <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[LR] /home/user/hmkdir4
2020/02/06 13:54:21.282104 127.0.0.1:50186 user[PAM] ListFilesRawFormat[LR] /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
--

```

4.2.23.9 StatLogPerUserInPrivilegeSeparation

```

=====
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
--

```

4.2.23.10 ApplicationStatLogSecurityEx

```

=====
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
--
```

4.2.24 System Operating Environment Settings, CPU Thread Control

4.2.24.1 MaxConcurrentThread

```
=====
Format : MaxConcurrentThread <max-threads>
-----
max-threads
Default : 0
Range of Values : signed integer
=====
```

The maximum number of threads is configured.

4.2.25 System Operating Environment Settings, Application Linked Function

4.2.25.1 CallbackScript

```
=====
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 by Archaea dialog).

- 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 by Archaea dialog file transfer operation)
- remove (API by Archaea dialog file removing operation)
- listraw (API by Archaea dialog file listing operation)
- mkd (API by Archaea dialog directory creation operation)
- pwd (API by Archaea dialog working directory printing operation)
- move (API by Archaea dialog file moving operation)
- link (API by Archaea dialog 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.param  
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
OK 0000 FT 00000001 /home/user/file_nodiskio_0
--

--
Example :
CallbackScript yes /var/tmp/hcp_callback.sh /var/tmp/hcp_callback
--

```

4.2.25.2 CallbackScriptHomeIsolation

```

=====
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
--
```

4.2.25.3 CallbackScriptNoSymbolicLink

```
=====
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
--
```

4.2.26 Others

4.2.26.1 EnsureDestinationInFileTransfer

```
=====
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  
--
```

5 Client Setup

5.1 Red Hat Enterprise Linux (RHEL)

5.1.1 Download RPM Package

Go to the following site and download the latest RPM package.

Download Site^{*1}

5.1.2 Installation of RPM Package

Install the package using rpm command.

```
rpm -ivh bytix-archaea-tools-1.5.0-35.el9.x86_64.rpm
```

That is all for fundamental setup of client commands.

This package installs hcp, hsync, hrm, hcp-ls, hmkdir, hpwd, hmv, hln, hchmod and hchown.

The old packages will be replaced as obsolete. Configuration files having some changes from the original one will be kept.

Please see the following page for fundamental operations to confirm if it works after the installation.

Here

5.1.3 Upgrade

To upgrade on Linux, you just run the RPM command with a newer package than the current version's package using -U option.

```
rpm -Uvh bytix-archaea-tools-1.5.0-35.el9.x86_64.rpm
```

Old configuration files will be kept. You can make upgrade even if using a newer package in build number.

Example: Upgrade from 1.5.0-34 to 1.5.0-35

1. <https://www.support.nec.co.jp/View.aspx?id=4140100145>

```
rpm -ivh bytix-archaea-tools-1.5.0-34.el9.x86_64.rpm
rpm -Uvh bytix-archaea-tools-1.5.0-35.el9.x86_64.rpm (this works)
```

5.1.4 Uninstallation

To uninstall on Linux, use -e option of the RPM command to do.

```
rpm -e bytix-archaea-tools
```

5.2 RPM Install the software into a non-default place

When installing, please specify the following options.

```
--relocate
--badreloc
```

Example:

```
[user@localhost ~]$ sudo rpm -ivh --relocate /=usr/local/archaea_tools --badreloc
bytix-archaea-tools-1.5.0-35.el9.x86_64.rpm
```

You can go to use clients without any such changes.

When uninstalling, you just make it in a normal way with specifying package names.

Do not specify --relocate and --badreloc.

Example:

```
[user@localhost ~]$ sudo rpm -e bytix-archaea-tools
```

When commands are installed on non-default place, their help options (-V) shows the following information about the place.

```
[user@localhost bin]$ ./hcp-ls -V
hcp-ls client (hcp-ls) 1.5.0_35 / Linux (HpFP2 2.0.0.91_21 WSAPI 0.0.1.30 WS 4.2.0-1)
Installed prefix: /usr/local/archaea_tools (/usr/local/archaea_tools/usr/bin/hcp-ls
)
```

In cases where any prefix is not detected.

```
[user@localhost temp_bin]$ ./hcp-ls -V
hcp-ls client (hcp-ls) 1.5.0_35 / Linux (HpFP2 2.0.0.91_21 WSAPI 0.0.1.30 WS 4.2.0-1)
Command placed at : /home/user/archaea_tools/temp_bin/hcp-ls
```

5.3 RPM Install the software by non-privileged users

When installing, please specify the following options.

```
--relocate
--badreloc
--nodeps
--dbpath
```

Installation registry information will be saved at the place specified by the --dbpath option that is a directory where you want to save the information.

Example:

```
[user@localhost ~]$ rpm -ivh --nodeps --dbpath=/home/user/rpm --relocate /=/home/user/archaea_tools --badreloc bytix-archaea-tools-1.5.0-35.el9.x86_64.rpm
```

When uninstalling, please specify the following options.

```
--nodeps
--dbpath
```

* Do not specify --relocate and --badreloc.

Example:

```
[user@localhost ~]$ rpm -e --nodeps --dbpath=/home/user/rpm bytix-archaea-tools
```

For clients, you need the following packages on your system.

```
libc, openssl, zlib
```

You can confirm them by --qa option of the rpm command.

Example:

```
[user@localhost ~]$ rpm -qa | grep -E -e "^(libicu|openssl|zlib)-"
libicu-67.1-9.el9.x86_64
openssl-pkcs11-0.4.11-7.el9.x86_64
libicu-devel-67.1-9.el9.x86_64
openssl-libs-3.0.1-43.el9_0.x86_64
openssl-devel-3.0.1-43.el9_0.x86_64
openssl-3.0.1-43.el9_0.x86_64
zlib-1.2.11-35.el9_1.x86_64
zlib-devel-1.2.11-35.el9_1.x86_64

[user@localhost ~]$ find /usr/lib64 | grep -E -e "^/usr/lib64/lib(icudata|icuuc|pam
|crypto|ssl|z)¥."
/usr/lib64/libicudata.so.67.1
/usr/lib64/libicudata.so.67
/usr/lib64/libz.so.1
/usr/lib64/libz.so.1.2.11
/usr/lib64/libicuuc.so.67
/usr/lib64/libicuuc.so.67.1
/usr/lib64/libcrypto.so.3
/usr/lib64/libcrypto.so.3.0.1
/usr/lib64/libssl.so.3
/usr/lib64/libssl.so.3.0.1
/usr/lib64/libpam.so.0.85.1
/usr/lib64/libpam.so.0
/usr/lib64/libcrypto.so
/usr/lib64/libz.so
/usr/lib64/libssl.so
/usr/lib64/libicudata.so
/usr/lib64/libicuuc.so
/usr/lib64/libpam.so
```

5.4 Confirm if It Works After Installation

Enter a command for Arcaea tools, e.g., `hcp-ls`, along with the host name or IP address of the server at a command prompt of a client computer. And then input your username and password, following interactive messages. Here is an example of the `hcp-ls` command to get a list of files and directories on the server.

```
[local_user@localhost ~]$ hcp-ls hcp.server.example.com
Login as:user //Enter your user name at hcp.server.example.com
user@hcp.server.example.com's password: // Enter a password of the user
```

```
// TODO list of files and directories
[local_user@localhost ~]$ echo $?
0 // The command which run is successfull.
```

In the same way, the `hcp` command can upload a local file to the home directory on the remote server.

```
[local_user@localhost ~]$ echo "The first remote copy example." > example.txt
[local_user@localhost ~]$ hcp example.txt hcp.server.example.com:example.txt
Login as:user
user@hcp.server.example.com's password:
[local_user@localhost ~]$ echo $?
0
```

The `hcp-ls` command shows the result of uploading. With the `-o` option, file attributes are also shown.

```
[local_user@localhost ~]$ hcp-ls -o "-l" hcp.server.example.com:example.txt
// Interactive text on the username and password omitted.
// TODO result
[local_user@localhost ~]$
```

Then you can also download the remote file at the server to another local file using the `hcp` command.

```
[local_user@localhost ~]$ hcp hcp.server.example.com:example.txt example.download.txt
// Interactive text on the username and password omitted.
[local_user@localhost ~]$ cat example.download.txt
The first remote copy example.
```

6 Client Commands

6.1 Client Command (hcp)

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

6.1.1 Basic Format

The basic format is as follows.

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

6.1.2 Option List

The options for the hcp commands are below.

Copy

Description	Short Name	Option Name
Keep source permission	p	<u>permission</u>
Recursive copy	R	<u>recursive</u>
Regular expression use (Wildcard exemption)	g	<u>regex</u>
Search any directories (Wildcard or regular expression is exempted)	Y	<u>anydirs</u>
Verify transfer data/files by the message digest	y	<u>verify</u>
Transmit compressed data blocks	z	<u>compress</u>
Resolve symbolic links (Dereference) and copy files	s	<u>copy-linkfile</u>
Resolve symbolic directory and copy files	S	<u>follow-linkdir</u>
resolve symbolic links specified on SOURCE to copy	H	<u>dereference-src</u>
Skip copying empty files	e	<u>no-emptyfile</u>
Skip copying empty directories	E	<u>no-emptydir</u>
Skip copying the files whose names start with '.'.	d	<u>no-dotfile</u>
Skip copying the directories whose names start with '.'.	D	<u>no-dotdir</u>
Copy the files with hidden attributes	l	<u>copy-hidden</u>
Copy the files with archive attributes	A	<u>archive-check</u>
Copy the files being aware of sparse files		<u>sparse</u>
Copy mode	m	<u>copy-mode</u>
Overwrite mode	o	<u>overwrite</u>
Specify how to behave when commands fail	a	<u>fail-action</u>
Sequentially read data with the read function (when a device file is specified as a source)		<u>reading-dev</u>
Read data of devices via Mapped I/O (when a device file is specified as a source)		<u>reading-dev-via-mmap</u>
Set the transfer expiration by second		<u>transfer-expire</u>
Control message out-of-order suppress mode		<u>no-out-of-order-header-messaging</u>
Disable skipping HCP files in transfer		<u>no-skip-hcp-file</u>
Disable ahead listing		<u>no-ahead-listing</u>
Specify a depth of the ahead listing		<u>ahead-listing-depth</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		<u>hpfp</u>
The port-separation UDP(HpFP) protocol(deprecated)		<u>udp</u>
Multiple connections		<u>mcd</u>

File I/O Extension Function

Description	Short Name	Option Name
Use file I/O extension (beta, Linux)		<u>fio-extension</u>
Use Direct I/O (beta, Linux)		<u>fio-direct</u>
Use Linux asynchronous I/O (beta, Linux)		<u>fio-async-linux</u>
Alignment size on Direct I/O		<u>fio-direct-align</u>
Alignment size on source site		<u>fio-direct-align-local</u>
Alignment size on destination site		<u>fio-direct-align-remote</u>
How to malloc with alignment		<u>fio-direct-malloc</u>
Reuse allocated memory with alignment		<u>fio-direct-reuse-aligned</u>
Threshold of files for Direct I/O		<u>fio-direct-threshold</u>
Maximum events of asynchronous I/O		<u>fio-async-max-events</u>
Maximum events to get on asynchronous I/O		<u>fio-async-max-get-events</u>
Timeout on getting events on asynchronous I/O		<u>fio-async-get-events-timeo</u>
How making pre-allocation of storage		<u>fio-fallocate</u>
Unit size of the pre-allocation		<u>fio-fallocate-unit</u>
Suppress file I/O extension on source site		<u>fio-no-extension-local</u>
Suppress file I/O extension on destination site		<u>fio-no-extension-remote</u>
Force file I/O extension for all files		<u>fio-extension-always</u>

Multiple File Batch Transfer Function

Description	Short Name	Option Name
Copy with a specified source file list	<u>f</u>	<u>source-file</u>
Set the remote host (in use of the source file)		<u>source-file-host</u>
Set the remote port (in use of the source file)		<u>port</u>

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		<u>hpfp-cong</u>

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		<u>hpfp-mss</u>

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		<u>hpfp-sndbuf</u>
Set the receiving buffer size for the HpFP protocol		<u>hpfp-rcvbuf</u>

Data Flow Control, Temporary File Save Function (Atomic File Save)

Description	Short Name	Option Name
Request for overwriting temporary files		<u>overwrite-als-temp-file</u>

Authentication

Description	Short Name	Option Name
Don't use agent		<u>no-agent</u>
Select identity		<u>ident-select</u>
Specify a username first and transfer		<u>user</u>
Specify a password first and transfer		<u>password</u>

Retransmission Function

Description	Short Name	Option Name
Resume the previous proceeding	r	<u>resume</u>
Automatically resume copying when it stops due to the network issues		<u>auto-resume</u>
Disable integrity check on resume		<u>no-integrity-on-resume</u>

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Performance Evaluation

Description	Short Name	Option Name
Measure disk I/O performance	N	<u>no-send</u>
Measure the network I/O performance of communication protocol	n	<u>no-diskio</u>
No disk I/O, but keep reading		<u>no-diskio-keep-read</u>
No disk I/O, but keep writing		<u>no-diskio-keep-write</u>
No disk I/O and Direct I/O, but keep malloc with alignment		<u>no-diskio-keep-memalign</u>

Display Control

Description	Short Name	Option Name
Specify an allowable short time to show the progress speed		<u>progress-speed-allow-short-time</u>

Log Management

Description	Short Name	Option Name
Suppress non-error messages	q	<u>quiet</u>
Specify an application diagnostic log output destination		<u>hcp-diag</u>
Specify various statistics log output destinations		<u>stat-log-file</u>
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		<u>multi-run</u>

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		<u>config-file</u>
Make configuration from command line		<u>config-option</u>
Show configuration option's names		<u>show-config-options</u>
Setting by a relative path from the current directory		<u>include-conf-from-cwd</u>
Server compatibility disabled		<u>no-earlier-serv-compat</u>

Check System Information

Description	Short Name	Option Name
Show system info		<u>system-info</u>
Run host benchmark		<u>run-host-benchmark</u>
Specify measurement categories on the benchmark		<u>run-host-benchmark-categories</u>

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

```
--investigation
```

6.1.3 Copy

6.1.3.1 p, permission

```
=====
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 ...
--
```

6.1.3.2 R, recursive

```
=====
Format : -R | --recursive
=====
```

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

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

6.1.3.3 g, regex

```
=====
Format : -g | --regex
=====
```

The path from source is regarded as a regular expression. The path from source is regarded as a pattern string in -cluding 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 ...
--
```

6.1.3.4 Y, anydirs

```
=====
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 ...  
--
```

6.1.3.5 y, verify

```
=====  
Format : -y | --verify  
=====
```

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

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

6.1.3.6 z, compress

```
=====  
Format : -z | --compress  
=====
```

Data blocks to send are compressed.

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

6.1.3.7 s, copy-linkfile

```
=====  
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 ...
--
```

6.1.3.8 S, follow-linkdir

```
=====
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 ...
--
```

6.1.3.9 H, dereference-src

```
=====
Format : -H | --dereference-src
=====
```

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

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

6.1.3.10 e, no-emptyfile

```
=====  
Format : -e | --no-emptyfile  
=====
```

hcp dose not copy empty files.

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

6.1.3.11 E, no-emptydir

```
=====  
Format : -E | --no-emptydir  
=====
```

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

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

6.1.3.12 d, no-dotfile

```
=====  
Format : -d | --no-dotfile  
=====
```

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

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

6.1.3.13 D, no-dotdir

```
=====
Format : -D | --no-dotdir
=====
```

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

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

6.1.3.14 I, copy-hidden

```
=====
Format : -I | --copy-hidden
=====
```

hcp copies hidden files.

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

6.1.3.15 A, archive-check

```
=====
Format : -A | --archive-check
=====
```

hcp copies files having archive attributes.

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

6.1.3.16 sparse

```
=====
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 ...
--
```

6.1.3.17 m, copy-mode

```
=====
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 ...
--
```

6.1.3.18 o, overwrite

```
=====
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 ...
--
```

6.1.3.19 a, fail-action

```
=====
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 ...
--
```

6.1.3.20 reading-dev

```
=====
Format : --reading-dev
=====
```

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

6.1.3.21 reading-dev-via-mmap

```
=====
Format : --reading-dev-via-mmap
=====
```

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

6.1.3.22 transfer-expire

```
=====
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.

6.1.3.23 no-out-of-order-header-messaging

```
=====
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.

6.1.3.24 no-skip-hcp-file

```
=====
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 : .hcp.out, .hcp.in, .hcp.diag, .hcp.statistics.*

6.1.3.25 no-ahead-listing

```
=====
Format : --no-ahead-listing
=====
```

This option disables the ahead listing that performs sending file requests in advance over the threshold of the application buffer size (determined by MaxBufferSize, etc) on the source of file transfers.

It is useful for reproducing the previous behavior to make troubleshooting of performance on your run-time environment.

6.1.3.26 ahead-listing-depth

```
=====
Format : --ahead-listing-depth=<depth-desc>
-----
depth-desc
Format : ( max | <decimal_number> | <decimal_number>[[(E|P|T|G|M|K)]B] | <decimal_n
umber>[[(E|P|T|G|M|K)]bit] )
Default : 200Gbit
Range of values : unsigned double-length integer
=====
```

This option tells a depth of the ahead listing by a number of files, data size or bandwidth. If you use a number of files, it will be rounded down to the limit (just under 50,000) in running time.

If you use 'max' (maximum depth), the ahead listing will be performed up to the limit.

It is useful for improving performance of file transfers when transferring many files. If RTT of an network environments is about from 500ms to 1s, the depth corresponding to the bandwidth is so optimal normally.

6.1.4 Selectable Communication Method Function

6.1.4.1 hpfp

```
=====
Format : --hpfp
=====
```

It instructs transport to use HpFP protocol.

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

6.1.4.2 udp

```
=====
Format : --udp=<hpfp_options>
  hpfp_options := <hpfp_udp_port>:<hpfp_cong_mode>:<hpfp_sndbuf>:<hpfp_rcvbuf>:<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)
  8MB (Raspbian)
Range of Values : unsigned double-length integer in byte. D stands for DEFAULT.
-----
hpfp_rcvbuf
Format : ( DEFAULT | D | <decimal_number>[[(T|G|M|K)]B] )
Default :
  200MB (Linux.x86)
  16MB (Raspbian)
Range of Values : unsigned double-length integer in byte. D stands for DEFAULT.
-----
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.

hpfp_cong_mode specifies congestion control mode.

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

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

The MSS (Maximum Segment Size) of the HpFP protocol is set in `hfp_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 ...
--
```

6.1.4.3 mcd

```
=====
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.

6.1.5 File I/O Extension Function

6.1.5.1 fio-extension

```
=====
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 --

6.1.5.2 fio-async-linux

```
=====
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-fallocatte option descibed below), resuming transfer (using the resume option) might starts 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
--
```

6.1.5.3 fio-direct

```
=====
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.dat
--
```

6.1.5.4 fio-direct-align

```
=====
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 ...
--
```

6.1.5.5 fio-direct-align-local

```
=====
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.

6.1.5.6 fio-direct-align-remote

```
=====
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.

6.1.5.7 fio-direct-malloc

```
=====
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.

6.1.5.8 fio-direct-reuse-aligned

```
=====
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 ...
--
```

6.1.5.9 fio-direct-threshold

```
=====
Format : --fio-direct-threshold=<file_size>
-----
file_size
Format : <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 ...
--
```

6.1.5.10 fio-async-max-events

```
=====
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 ...
--
```

6.1.5.11 fio-async-max-get-events

```
=====
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 ...
--
```

6.1.5.12 fio-async-get-events-timeo

```
=====
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 ... // timeout of 1 m
illiseconds
--
```

6.1.5.13 fio-fallocate

```
=====
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 ...  
--
```

6.1.5.14 fio-fallocate-unit

```
=====  
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 ...  
--
```

6.1.5.15 fio-no-extension-local

```
=====  
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 ...
--
```

6.1.5.16 fio-no-extension-remote

```
=====
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 ...
--
```

6.1.5.17 fio-extension-always

```
=====
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 ...
--
```

6.1.6 Multiple File Batch Transfer Function

6.1.6.1 f, source-file

```
=====
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_dir/
192.168.100.100:874:/home/user/file3.txt

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

6.1.6.2 source-file-host

```
=====
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 ...
--
```

6.1.6.3 port

```
=====
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 ...
--
```

6.1.7 Congestion Control

6.1.7.1 hpfp-cong

```
=====
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 192.168.10.100:65520:/path/to/dst_file
--
```

6.1.8 Data Flow Control, Message Data Size Control

6.1.8.1 hpfp-mss

```
=====
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
--
```

6.1.9 Data Flow Control, Data Buffer Setting

6.1.9.1 hpfp-sndbuf

```
=====
Format : --hpfp-sndbuf=<hpfp_sndbuf>
-----
hpfp_sndbuf
Format : <decimal_number>[[(T|G|M|K)]B]
Default :
    100MB (Linux.x86)
    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 ... --hfp --hfp-sndbuf=8MB /path/to/src_file 192.168.10.1
00:65520:/path/to/dst_file
--
```

6.1.9.2 hfp-rcvbuf

```
=====
Format : --hfp-rcvbuf=<hfp_rcvbuf>
-----
hfp_rcvbuf
Format : <decimal_number>[[ (T|M|K)]B]
Default :
    200MB (Linux.x86)
    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 192.168.10.
100:65520:/path/to/dst_file
--
```

6.1.10 Data Flow Control, Temporary File Save Function (Atomic File Save)

6.1.10.1 overwrite-als-temp-file

```
=====
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.

6.1.11 Authentication

6.1.11.1 no-agent

```
=====
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.

6.1.11.2 ident-select

```
=====
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.

6.1.11.3 user

```
=====
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 ...
--
```

6.1.11.4 password

```
=====
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 ...
--
```

6.1.12 Retransmission Function

6.1.12.1 r, resume

```
=====
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`.

6.1.12.2 auto-resume

```
=====
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.

6.1.12.3 no-integrity-on-resume

```
=====
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

6.1.13 Performance Evaluation

6.1.13.1 N, no-send

```
=====
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 ...
--
```

6.1.13.2 n, no-diskio

```
=====
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/null
--
```

6.1.13.3 no-diskio-keep-read

```
=====
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.

6.1.13.4 no-diskio-keep-write

```
=====
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.

6.1.13.5 no-diskio-keep-memalign

```
=====
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.

6.1.14 Display Control

6.1.14.1 progress-speed-allow-short-time

```
=====
Format : --progress-speed-allow-short-time=<time_desc>
-----
time-desc
Format : ( <decimal_number>[(usec|us|msec|ms)] )
Default : 100usec
Range of values : 1 - 100000 (100 milliseconds)
=====
```

This option tells a threshold time to use the unknown description for the speed description in the progress of file transfers that will be applied when its measurement intervals are short.

6.1.15 Log Management

6.1.15.1 q, quiet

```
=====
Format : -q | --quiet
=====
```

Suppress non-error message outputs.

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

6.1.15.2 hcp-diag

```
=====
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.

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

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

6.1.15.3 stat-log-file

```
=====
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.

```

<configured path>.application (application statistics)
<configured path>.transport.tcp (TCP transport statistics)
<configured path>.transport.hpfp (HpFP transport statistics)

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

```

6.1.15.4 hcp-out

```

=====
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
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)
```

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, 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\
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>
```

6.1.15.5 multi-run

```

=====
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.
--
```

6.1.16 Software Information Update

6.1.16.1 V, version

```
=====
Format : -V | --version
=====
```

The hcp command version is shown.

```
--
Example:
[user@localhost ~]$ hcp -V
hcp client (hcp) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

6.1.16.2 config-test

```
=====
Format : --config-test
=====
```

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_ed25
519 ~/.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/CB
C [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).

6.1.16.3 h, help

```

=====
Format : -h | --help
=====

```

The help information on the hcp commands is shown.

```

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

```

6.1.17 System Operating Environment Settings

6.1.17.1 config-file

```
=====
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 ...
--
```

6.1.17.2 config-option

```
=====
Format : --config-option=<config-file-option-desc>
-----
config-file-option-desc
Default : none
Range of Values : description of a configuration item described in configuration 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" ...  
--
```

6.1.17.3 show-config-options

```
=====  
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 ...  
--
```

6.1.17.4 include-conf-from-cwd

```
=====  
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.

6.1.17.5 no-earlier-serv-compat

```
=====  
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 Server backward compatibility conditions list in the back of this document about what conditions the function works in.

6.1.18 Check System Information

6.1.18.1 system-info

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

6.1.18.2 run-host-benchmark

```
=====
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 ...
--
```

6.1.18.3 run-host-benchmark-categories

```
=====
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 ...
--
```

6.2 Client Command (hsync)

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

6.2.1 Basic Format

The basic format is as follows.

```
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
```

6.2.2 Option List

The options for the hsync commands are below.

Synchronization

Description	Short Name	Option Name
Verify transferred files by digest check	c	<u>checksum</u>
Archive mode is -rlptgoD	a	<u>archive</u>
Recurse into directories	r	<u>recursive</u>
Use relative path names	R	<u>relative</u>
Don't send implied dirs with --relative		<u>no-implied-dirs</u>
Make backups	b	<u>backup</u>
Make backups into hierarchy based in DIR		<u>backup-dir</u>
Backup suffix (default ~)		<u>suffix</u>
New files are updated	u	<u>update</u>
Update destination files by in-place copy		<u>inplace</u>
Transfer directories without recursing	d	<u>dirs</u>
Copy symlinks as symlinks	l	<u>links</u>
Transform symlink into referent file/dir	L	<u>copy-links</u>
Only "unsafe" symlinks are transformed		<u>copy-unsafe-links</u>
Ignore symlinks that point outside the tree		<u>safe-links</u>
Transform symlink to dir into referent dir	k	<u>copy-dirlinks</u>
Treat symlinked dir on receiver as dir	K	<u>keep-dirlinks</u>
Preserve permissions	p	<u>perms</u>
Preserve executability	E	<u>executability</u>
Affect file and/or directory permissions		<u>chmod</u>
Preserve owner	o	<u>owner</u>
Preserve group	g	<u>group</u>
Preserve device files		<u>devices</u>
Preserve special files		<u>specials</u>
Specify device files and special files	<u>D</u>	
Preserve modification times	t	<u>times</u>
Omit directories from --times	O	<u>omit-dir-times</u>
Omit symlinks from --times	J	<u>omit-link-times</u>
Receiver attempts super-user activities		<u>super</u>
Turn sequences of nulls into sparse blocks		sparse
Copy files whole	W	<u>whole-file</u>
Copy over one file system		<u>one-file-system</u>
Skip creating new files on receiver		<u>existing</u>

Description	Short Name	Option Name
Skip updating files that exist on receiver		<u>ignore-existing</u>
An alias for --delete-during		<u>del</u>
Delete extraneous files from dest dirs		<u>delete</u>
Receiver deletes before transfer, not during		<u>delete-before</u>
Receiver deletes during the transfer		<u>delete-during</u>
Find deletions during, delete after transfer		<u>delete-delay</u>
Receiver deletes after transfer, not during		<u>delete-after</u>
Delete excluded files from dest dirs		<u>delete-excluded</u>
Force deletion of dirs even if not empty		<u>force</u>
Don't delete more than NUM files		<u>max-delete</u>
Don't transfer any file larger than SIZE		<u>max-size</u>
Don't transfer any file smaller than SIZE		<u>min-size</u>
Keep partially transferred files		<u>partial</u>
Put a partially transferred file into DIR		<u>partial-dir</u>
Prune empty directory chains from file-list	m	<u>prune-empty-dirs</u>
Don't map uid/gid values by user/group name		<u>numeric-ids</u>
Custom username mapping		<u>usermap</u>
Custom groupname mapping		<u>groupmap</u>
Simple username/groupname mapping		<u>chown</u>
Don't skip files that match size and time	l	<u>ignore-times</u>
Skip files that match in size		<u>size-only</u>
Set the accuracy for mod-time comparisons	@	<u>modify-window</u>
Create temporary files in directory DIR	T	<u>temp-dir</u>
Compress file data during the transfer	z	<u>compress</u>
Explicitly set compression level		<u>compress-level</u>
Exclude HCP files from transfer		<u>hcp-exclude</u>
Add a file-filtering	f	<u>filter</u>
Add a rule to exclude files		<u>exclude</u>
Read exclude patterns from a file		<u>exclude-from</u>
Add a rule to include files		<u>include</u>
Read include patterns from a file		<u>include-from</u>
Read a list of source-file names from a file		<u>files-from</u>
Give some file-transfer stats		<u>stats</u>

Description	Short Name	Option Name
Output numbers in a human-readable format	h	<u>human-readable</u>
Show progress during transfer		<u>progress</u>
Specify partial and progress settings	<u>P</u>	
Output a change-summary for all updates	i	<u>itemize-changes</u>
Output updates using the specified format		<u>out-format</u>
Stop rsync at the specified point in time		<u>stop-at</u>
Stop rsync after the specified time have elapsed		<u>stop-after</u>
Disable ahead listing		no-ahead-listing
Specify a depth of the ahead listing		ahead-listing-depth

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp
Multiple connections		mcd

File I/O Extension Function

Description	Short Name	Option Name
Use file I/O extension (beta, Linux)		fio-extension
Use Direct I/O (beta, Linux)		fio-direct
Use Linux asynchronous I/O (beta, Linux)		fio-async-linux
Alignment size on Direct I/O		fio-direct-align
Alignment size on source site		fio-direct-align-local
Alignment size on destination site		fio-direct-align-remote
How to malloc with alignment		fio-direct-malloc
Reuse allocated memory with alignment		fio-direct-reuse-aligned
Threshold of files for Direct I/O		fio-direct-threshold
Maximum events of asynchronous I/O		fio-async-max-events
Maximum events to get on asynchronous I/O		fio-async-max-get-events
Timeout on getting events on asynchronous I/O		fio-async-get-events-timeo
How making pre-allocation of storage		fio-fallocate
Unit size of the pre-allocation		fio-fallocate-unit
Suppress file I/O extension on source site		fio-no-extension-local
Suppress file I/O extension on destination site		fio-no-extension-remote
Force file I/O extension for all files		fio-extension-always

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hpfp-rcvbuf

Data Flow Control, Bandwidth Control

Description	Short Name	Option Name
Limit socket I/O bandwidth		<u>bwlimit</u>

Authentication

Description	Short Name	Option Name
Specify a username first and synchronization		user
Specify a password first and synchronization		password

Retransmission Function

Description	Short Name	Option Name
Automatically rerun		<u>auto-rerun</u>

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Performance Evaluation

Description	Short Name	Option Name
Perform a trial run with no changes made	n	<u>dry-run</u>
No disk I/O, but keep reading		dry-run-keep-read
No disk I/O, but keep writing		dry-run-keep-write
No disk I/O and Direct I/O, but keep malloc with alignment		dry-run-keep-memalign

Display Control

Description	Short Name	Option Name
Specify an allowable short time to show the progress speed		progress-speed-allow-short-time

Log Management

Description	Short Name	Option Name
Increase log verbosity	v	<u>verbose</u>
Set the log verbosity level of INFO		<u>info</u>
Suppress non-error messages	q	<u>quiet</u>
Specify a file where to log progress		<u>log-file</u>
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		hcp-stat-log-file
Specify an execution record output destination		hcp-out
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpf, --fio-extension, --fio-direct, --fio-async-linux, --sparse, --user, --password, --config-file, --config-option, --show-config-options, --system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, --hcp-stat-log-file, --udp, --hpf-cong, --hpf-mss, --hpf-sndbuf, --hpf-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-ahead-listing, --ahead-listing-depth, --progress-speed-allow-short-time, --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.

6.2.3 Synchronization

6.2.3.1 c, checksum

```
=====
Format : -c | --checksum
=====
```

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

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

6.2.3.2 a, archive

```
=====
Format : -a | --archive
=====
```

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

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

6.2.3.3 r, recursive

```
=====
Format : -r | --recursive
=====
```

It recursively searches directories and transmits files.

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

6.2.3.4 R, relative

```
=====
Format : -R | --relative
=====
```

Use relative paths.

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

6.2.3.5 no-implied-dirs

```
=====
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 ...
--
```

6.2.3.6 b, backup

```
=====
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 ...
--
```

6.2.3.7 backup-dir

```
=====
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 ...
--
```

6.2.3.8 suffix

```
=====
Format : --suffix=<suffix-name>
=====
```

The suffix to rename for backup is specified.

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

6.2.3.9 u, update

```
=====
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 ...
--
```

6.2.3.10 inplace

```
=====
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 ...
--
```

6.2.3.11 d, dirs

```
=====
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
--
```

6.2.3.12 l, links

```
=====
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 ...  
--
```

6.2.3.13 L, copy-links

```
=====  
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 ...  
--
```

6.2.3.14 copy-unsafe-links

```
=====  
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 ... --

6.2.3.15 safe-links

```
=====
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 ...
--
```

6.2.3.16 k, copy-dirlinks

```
=====
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 ...
--
```

6.2.3.17 K, keep-dirlinks

```
=====
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 ...
--
```

6.2.3.18 p, perms

```
=====
Format : -p | --perms
=====
```

The source permissions are maintained at the destination when copying.

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

6.2.3.19 E, executability

```
=====
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 ...

6.2.3.20 chmod

```
=====
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 ...
--
```

6.2.3.21 o, owner

```
=====
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 ...
--
```

6.2.3.22 g, group

```
=====
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 ...
--
```

6.2.3.23 devices

```
=====
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 ...
--
```

6.2.3.24 specials

```
=====
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 ...
--
```

6.2.3.25 D

```
=====
Format : -D
=====
```

This tells hsync to use --devices and --specials.

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

6.2.3.26 t, times

```
=====
Format : -t | --times
=====
```

This option maintains the modification time of the source file.

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

6.2.3.27 O, omit-dir-times

```
=====
Format : -O | --omit-dir-times
=====
```

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

This option is effective only when both `-r` and `--times` options are enabled. This option is also applied to symbolic links to directories. The update time is not stored.

```
--
Example:
[user@localhost ~]$ hsync -rt0 ...
--
```

6.2.3.28 J, omit-link-times

```
=====
Format : -J | --omit-link-times
=====
```

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

This option is effective only when both `--times` and `--links` options are enabled.

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

6.2.3.29 super

```
=====
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 ...
--
```

6.2.3.30 n, dry-run

```
=====
Format : -n | --dry-run
=====
```

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

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

6.2.3.31 W, whole-file

```
=====
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. This option is effective only when --inplace options are enabled.

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

6.2.3.32 one-file-system

```
=====
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 ...
--
```

6.2.3.33 existing

```
=====
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 ...
--
```

6.2.3.34 ignore-existing

```
=====
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 ...
--
```

6.2.3.35 del

```
=====
Format : --del
=====
```

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

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

6.2.3.36 delete

```
=====
Format : --delete
=====
```

This option deletes files and directories in the destination that don't exist in the source. The deletion range is confined to the synchronized directories.

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

6.2.3.37 delete-before

```
=====
Format : --delete-before
=====
```

This option requests file deletions be executed before the transfer.

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

6.2.3.38 delete-during

```
=====
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 ...
--
```

6.2.3.39 delete-delay

```
=====
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 ...
--
```

6.2.3.40 delete-after

```
=====
Format : --delete-after
=====
```

This option requests file deletions be executed after the transfer.

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

6.2.3.41 delete-excluded

```
=====
Format : --delete-excluded
=====
```

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

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

6.2.3.42 force

```
=====
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 ...
--
```

6.2.3.43 max-delete

```
=====
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 ...
--
```

6.2.3.44 max-size

```
=====
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 ... --

6.2.3.45 min-size

```
=====
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 ...
--
```

6.2.3.46 partial

```
=====
Format : --partial
=====
```

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

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

6.2.3.47 partial-dir

```
=====
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_ ...
--
```

6.2.3.48 m, prune-empty-dirs

```
=====
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 ...
--
```

6.2.3.49 numeric-ids

```
=====
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 -o -g --numeric-ids ...
--
```

6.2.3.50 usermap

```
=====
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 -o --usermap=0-99:nobody,wayne:admin,*:normal ...
--
```

6.2.3.51 groupmap

```
=====
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 -g --groupmap=usr:1,1:usr ...
--
```

6.2.3.52 chown

```
=====
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 ...
```

6.2.3.53 I, ignore-times

```
=====
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 ...
--
```

6.2.3.54 size-only

```
=====
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 ...
--
```

6.2.3.55 @, modify-window

```
=====
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 it will be
decided as same files in time.
--
```

6.2.3.56 T, temp-dir

```
=====
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:/pat
h/to/dst
// /path/to/dst/_temp_dir_ is the temporary directory of this transfer.
Example2:
[user@localhost ~]$ hsync --temp-dir=/home/user/_temp_dir_ ...
--
```

6.2.3.57 z, compress

```
=====  
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 ...  
--
```

6.2.3.58 compress-level

```
=====  
Format : --compress-level=<level>  
-----  
level  
Default : 5  
Range of Values : 0 - 9  
=====
```

It set the compress level.

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

6.2.3.59 hcp-exclude

```
=====  
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 : .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.

```
--
Example1:
[user@localhost ~]$ hsync --hcp-exclude ...
Example2:
[user@localhost ~]$ hsync --filter="-H" ...
--
```

6.2.3.60 f, filter

```
=====
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 [--hxp-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="" ... --

6.2.3.61 exclude

```
=====
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" ...
--
```

6.2.3.62 exclude-from

```
=====
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 ~]$ rsync --include="*/" --include="*.c" --exclude-from=".exclude-r
ule" ...
--
```

6.2.3.63 include

```
=====
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" ...
--
```

6.2.3.64 include-from

```
=====
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="*" ...
--
```

6.2.3.65 files-from

```
=====
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 ...
--
```

6.2.3.66 stats

```
=====
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 ...
--
```

6.2.3.67 h, human-readable

```
=====
Format : -h | --human-readable
=====
```

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

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

6.2.3.68 progress

```
=====
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 ...
--
```

6.2.3.69 P

```
=====
Format : -P
=====
```

This tells hsync to enable --partial and --progress.

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

6.2.3.70 i, itemize-changes

```
=====  
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 ...  
--
```

6.2.3.71 out-format

```
=====  
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" ... --

6.2.3.72 stop-at

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

6.2.3.73 stop-after

```
=====
Format : --stop-after=<mins-desc>
-----
mins-desc
Default : -1
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 ...
--
```

6.2.4 Data Flow Control, Bandwidth Control

6.2.4.1 bwlimit

```
=====
Format : --bwlimit=<bw-desc>
-----
bw-desc
Default : none
Range of Values : numeric value (byte), throughput string with unit (byte)
=====
```

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 ...
--
```

6.2.5 Retransmission Function

6.2.5.1 auto-rerun

```
=====
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 AutoRerunTrials is unlimited and you use 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 makes a cache on the memory of that passphrase to prevent interactive prompts from being shown for re-authentication.

6.2.6 Log Management

6.2.6.1 v, verbose

```
=====
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 ...
--
```

6.2.6.2 info

6.2.6.3 q, quiet

```
=====
Format : -q | --quiet
=====
```

Suppress non-error message outputs.

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

6.2.6.4 log-file

```
=====
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" ...
--
```

6.2.7 Software Information Update

6.2.7.1 V, version

```
=====
Format : -V | --version
=====
```

The hsync command version is shown.

```
--
Example:
[user@localhost ~]$ hsync -V
hsync client (hsync) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2
)
--
```

6.2.7.2 config-test

```
=====
Format : --config-test
=====
```

The hsync command parameters and configuration parameters are shown.

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

-- [Sources] -----
-- [Destination] -----
-- [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
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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.2.7.3 h, help

```

=====
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
--

```

6.3 Client Command (hrm)

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

6.3.1 Basic Format

The basic format is as follows.

```

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

```

6.3.2 Option List

The options for the hrm commands are below.

Deletion

Description	Short Name	Option Name
Delete the file without showing the confirmation message.	f	<u>force</u>
Delete the file recursively	R	<u>recursive</u>
Delete the empty directory.	d	<u>dir</u>
Show the confirmation message at each deletion.	i	
Show the confirmation message just once at the first deletion.	l	
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hpfp-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and deletion		user
Specify a password first and deletion		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Performance Evaluation

Description	Short Name	Option Name
Measure network I/O performance with HCP protocol	n	no-diskio

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,  
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -  
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mul  
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele  
ct
```

6.3.3 Deletion

6.3.3.1 f, force

```
=====  
Format : -f | --force  
=====
```

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

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

6.3.3.2 R, recursive

```
=====
Format : -R | --recursive
=====
```

Files are deleted recursively.

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

6.3.3.3 d, dir

```
=====
Format : -d | --dir
=====
```

Even empty directories are deleted.

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

6.3.3.4 i

```
=====
Format : -i
=====
```

The confirmation message is shown at each deletion.

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

6.3.3.5 I

```
=====
Format : -I
=====
```

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

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

6.3.3.6 host

```
=====
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 deletion target. With this parameter, the host name can be abbreviated.

```
--
Example:
[user@localhost ~]$ hrm --host=192.168.100.100 ...
--
```

6.3.3.7 port

```
=====
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 ...  
--
```

6.3.4 Log Management

6.3.4.1 hcp-out

```
=====  
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 ./  
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=- ...  
--
```

6.3.5 Software Information Update

6.3.5.1 V, version

```
=====
Format : -V | --version
=====
```

Show the hrm command version.

```
--
Example:
[user@localhost ~]$ hrm -V
hrm client (hrm) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

6.3.5.2 config-test

```
=====
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
WinLogonUserAuthentication : yes
PAMAuthentication        : yes
LocalPasswordAuthentication : yes
NumberOfPasswordPrompts   : 3
CompressLevel             : -1
StrictHostKeyChecking     : ask
IdentityFile              : - [~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.3.5.3 h, help

```

=====
Format : -h | --help
=====

```

The help for the hrm commands are shown.

```

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

```

6.4 Client Command (hcp-ls)

The hcp-ls command gets the file list on the remote servers (server or hcpd server).

6.4.1 Basic Format

The basic format is as follows.

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

6.4.2 Option List

The options for the hcp-ls commands are below.

File List Acquisition

Description	Short Name	Option Name
Set the flag to query command names	q	<u>query-cmdname</u>
Set the command option	o	<u>cmd-options</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpf-p-sndbuf
Set the receiving buffer size for the HpFP protocol		hpf-p-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and file list acquisition		user
Specify a password first and file list acquisition		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file,--udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mult
i-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-selec
t
```

6.4.3 File List Acquisition

6.4.3.1 q, query-cmdname

```
=====
Format : -q | --query-cmdname
=====
```

Command names on the command list operated on servers are queried. Either of the following commands is shown.

- ls (Linux)

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

6.4.3.2 o, cmd-options

```
=====
Format : -o <options> | --cmd-options=<options>
-----
options
Default : none
Range of Values : parameter option for the ls command.
=====
```

The command options are set. When they include the blank or “-”, it should be quote.

```
--
Example:
[user@localhost ~]$ hcp-ls -o "-al" ...
--
```

6.4.3.3 host

```
=====
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 ...
--
```

6.4.3.4 port

```
=====
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.

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

6.4.4 Log Management

6.4.4.1 hcp-out

```
=====
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=- ...
--
```

6.4.5 Software Information Update

6.4.5.1 V, version

```
=====
Format : -V | --version
=====
```

The hcp-ls command version is shown.

```
--
Example:
[user@localhost ~]$ hcp-ls -V
hcp-ls client (hcp-ls) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0
-2)
--
```

6.4.5.2 config-test

```
=====
Format : --config-test
=====
```

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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.4.5.3 h, help

```

=====
Format : -h | --help
=====

```

The hcp-ls command help line is shown.

```
--
Example:
[user@localhost ~]$ hcp-ls -h
--
```

6.5 Client Command (hmkdir)

The mkdir command creates directories on the remote servers (server or hcpd server).

6.5.1 Basic Format

The basic format is as follows.

```
Usage: mkdir [OPTION]... [USER@]HOST[:PORT]:DIRECTORY [:DIRECTORY]...
or: mkdir [OPTION]... --host=HOST [--port=PORT] [--user=USER] DIRECTORY...
```

6.5.2 Option List

The options for the mkdir commands are below.

Directory Creating

Description	Short Name	Option Name
Set the flag to create parents directory	p	<u>parents</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hfp-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and directory creating		user
Specify a password first and directory creating		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mul
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele
ct
```

6.5.3 Directory Creating

6.5.3.1 p, parents

```
=====
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 happens when the parent directory dose not exist.

```
--
Example:
[user@localhost ~]$ hmdir -p ...
--
```

6.5.3.2 host

```
=====
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
--
```

6.5.3.3 port

```
=====
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 ~]$ hmdir --port=1874
--
```

6.5.4 Log Management

6.5.4.1 hcp-out

```
=====
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 ~]$ hmdir --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 ~]$ hmdir --hcp-out=- ...
--
```

6.5.5 Software Information Update

6.5.5.1 V, version

```
=====
Format : -V | --version
=====
```

Show the hmdir command version.

```
--
Example:
[user@localhost ~]$ hmdir -V
hmdir client (hmdir) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0
-2)
--
```

6.5.5.2 config-test

```
=====
Format : --config-test
=====
```

Display the input parameters for the hmdir command and the configuration information.

```
--
Example:
[user@localhost ~]$ hmdir --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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.5.5.3 h, help

```

=====
Format : -h | --help
=====

```

Show the hmkdir command line help.

```

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

```

6.6 Client Command (hpwd)

The hpwd command shows working directories on the remote server (server or hcpd server).

6.6.1 Basic Format

The basic format is as follows.

```
Usage: hpwd [OPTION]... [USER@]HOST[:PORT]
```

6.6.2 Option List

The options for the hpwd commands are below.

Showing the Current Working Directory

Description	Short Name	Option Name
Logical path	L	<u>logical</u>
Physical path	P	<u>physical</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hpfp-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and showing the current working directory		user
Specify a password first and showing the current working directory		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mul
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele
ct
```

6.6.3 Showing the Current Working Directory

6.6.3.1 L, logical

```
=====
Format : -L | --logical
=====
```

The logical path is returned.

```
--
Example:
[user@localhost ~]$ hpwd -L ...
--
```

6.6.3.2 P, physical

```
=====
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 ...
--
```

6.6.4 Software Information Update

6.6.4.1 V, version

```
=====
Format : -V | --version
=====
```

The hpwd command version is shown.

```
--
Example:
[user@localhost ~]$ hpwd -V
hpwd client (hpwd) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

6.6.4.2 config-test

```
=====
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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.6.4.3 h, help

```

=====
Format : -h | --help
=====

```

Show the hpwd command line help.

```

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

```

6.7 Client Command (hmv)

The hmv commands are used to transfer files or directories to and from the remote server or hcpd server.

6.7.1 Basic Format

The basic format is as follows.

```
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
or: hmv [OPTION]... --host=HOST [--port=PORT] [--user=USER] SOURCE... DIRECTORY
```

6.7.2 Option List

The options for the hmv commands are below.

File Move

Description	Short Name	Option Name
Force overwriting in the destination	f	<u>force</u>
Interactive overwriting in the destination	i	<u>interactive</u>
Prohibited overwriting in the destination	N	<u>no-overwrite</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpf-p-sndbuf
Set the receiving buffer size for the HpFP protocol		hpf-p-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and file move		user
Specify a password first and file move		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpf, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file, --udp, --hpf-cong, --hpf-mss, --hpf-sndbuf, --hpf-rcvbuf, --mul
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele
ct
```

6.7.3 File Move

6.7.3.1 f, force

```
=====
Format : -f | --force
=====
```

When the same file or directory exists in the destination, it is overwritten.

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

6.7.3.2 i, interactive

```
=====
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 ...
--
```

6.7.3.3 N, no-overwrite

```
=====
Format : -N | --no-overwrite
=====
```

When the same file or directory exists in the destination, the process is skipped without overwriting.

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

6.7.3.4 host

```
=====
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 ...
--
```

6.7.3.5 port

```
=====
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 ...
--
```

6.7.4 Log Management

6.7.4.1 hcp-out

```
=====
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=- ...
--
```

6.7.5 Software Information Update

6.7.5.1 V, version

```
=====
Format : -V | --version
=====
```

The hmv command version is shown.

```
--
Example:
[user@localhost ~]$ hmv -V
hmv client (hmv) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

6.7.5.2 config-test

```
=====
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       : -
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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.7.5.3 h, help

```

=====
Format : -h | --help
=====

```

The hmv command help is shown.

```

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

```

6.8 Client Command (hln)

The hln commands creates links for the files and directories on the remote server and hcpd server.

6.8.1 Basic Format

The basic format is as follows.

```

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 LINK_NAME
or: hln [OPTION]... --host=HOST [--port=PORT] [--user=USER] TARGET... DIRECTORY

```

6.8.2 Option List

The options for the hln commands are below.

Link Creating

Description	Short Name	Option Name
Force overwriting in the destination	f	<u>force</u>
Interactive overwriting in the destination	i	<u>interactive</u>
Disable the dereference of the directory for the symbolic link	N	<u>no-dereference</u>
Create symboloc link	s	<u>symbolic</u>
Use the target path as a logic name (symbolic link is resolved)	L	<u>logical</u>
Use the target path as a logic name (symbolic link isn't resolved)	P	<u>physical</u>
expand the target's relative path to an absolute path		<u>symlink-target-expand-relative</u>
accept the target expansion (when server is an older versin)		<u>symlink-target-accept-expand-relative</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpf-p-sndbuf
Set the receiving buffer size for the HpFP protocol		hpf-p-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and link creating		user
Specify a password first and link creating		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mul
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele
ct
```

6.8.3 Link Creating

6.8.3.1 f, force

```
=====
Format : -f | --force
=====
```

When the same link exists in the destination, it is supposed to be overwritten without confirmation.

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

6.8.3.2 i, interactive

```
=====
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 ...
--
```

6.8.3.3 N, no-dereference

```
=====
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 ...
--
```

6.8.3.4 s, symbolic

```
=====
Format : -s | --symbolic
=====
```

Symbolic links will be created instead of hard links.

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

6.8.3.5 L, logical

```
=====  
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 ...  
--
```

6.8.3.6 P, physical

```
=====  
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 ...  
--
```

6.8.3.7 symlink-target-expand-relative

```
=====
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 ...
--
```

6.8.3.8 symlink-target-accept-expand-relative

```
=====
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 work when the server is an old one and it does 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 ...
--
```

6.8.3.9 host

```
=====
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 ...
--
```

6.8.3.10 port

```
=====
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 ...
--
```

6.8.4 Log Management

6.8.4.1 hcp-out

```
=====
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=- ...
--
```

6.8.5 Software Information Update

6.8.5.1 V, version

```
=====
Format : -V | --version
=====
```

The hln command version is shown.

```
--
Example:
[user@localhost ~]$ hln -V
hln client (hln) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0-2)
--
```

6.8.5.2 config-test

```
=====
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 ~/.ssh/id_ed25
519 ~/.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/CB
```

```

C [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.
--

```

6.8.5.3 h, help

```

=====
Format : -h | --help
=====

```

The hln command help is shown.

```

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

```

6.9 Client Command (hchmod)

The hchmod command is a command to change permissions of files on the server.

6.9.1 Basic Format

The basic format is as follows.

```

Usage: hchmod [OPTION]... MODE[,MODE...] [USER@]HOST[:PORT]:FILE [:FILE]...
or: hchmod [OPTION]... OCTAL-MODE [USER@]HOST[:PORT]:FILE [:FILE]...
or: hchmod [OPTION]... --host=HOST [--port=PORT] [--user=USER] MODE[,MODE...] FI
LE...
or: hchmod [OPTION]... --host=HOST [--port=PORT] [--user=USER] OCTAL-MODE FILE..
.

```

6.9.2 Option List

The options for the hcchmod commands are below.

Permission Change

Description	Short Name	Option Name
Change recursively	R	<u>recursive</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hpfp-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and permission change		user
Specify a password first and permission change		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,  
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -  
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mu  
lti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sel  
ect
```

6.9.3 Permission Change

6.9.3.1 R, recursive

```
=====  
Format : -R | --recursive  
=====
```

Changes permissions traversing directories recursively.

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

6.9.3.2 host

```
=====  
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 ...
--
```

6.9.3.3 port

```
=====
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 ...
--
```

6.9.4 Log Management

6.9.4.1 hcp-out

```
=====
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=- ...
--

```

6.9.5 Software Information Update

6.9.5.1 V, version

```

=====
Format : -V | --version
=====

```

The hchmod command version is shown.

```

--
Example:
[user@localhost ~]$ hchmod -V
hchmod client (hchmod) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0
-2)
--

```

6.9.5.2 config-test

```

=====
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
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 ~/.ssh/id_ed25
519 ~/.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/CB
C [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.
--

```

6.9.5.3 h, help

```

=====
Format : -h | --help
=====

```

The hchmod command help is shown.

```
--
Example:
[user@localhost ~]$ hchmod -h
--
```

6.10 Client Command (hchown)

The hchown command is a command to change owner or group of files on the server. The user ownership is specified by username and user ID, and the group ownership is by group name and group ID.

6.10.1 Basic Format

The basic format is as follows.

```
Usage: hchown [OPTION]... OWNER[:[GROUP]] [USER@]HOST[:PORT]:FILE [:FILE]...
      or: hchown [OPTION]... --host=HOST [--port=PORT] [--user=USER] OWNER[:[GROUP]] F
      ILE...
```

6.10.2 Option List

The options for the hchown commands are below.

Ownership Change

Description	Short Name	Option Name
Disable the dereference of the symbolic link	d	<u>no-dereference</u>
Change recursively	R	<u>recursive</u>
Follow symbolic links to directories on command line	s	<u>follow-cmd-link-dir</u>
Follow all symbolic links	S	<u>follow-all</u>
No follow symbolic links	D	<u>no-follow</u>
Set the remote host		<u>host</u>
Set the remote port		<u>port</u>

Selectable Communication Method Function

Description	Short Name	Option Name
The HpFP protocol		hpfp
The port-separation UDP(HpFP) protocol(deprecated)		udp

Congestion Control

Description	Short Name	Option Name
Congestion control modes in the HpFP protocol		hpfp-cong

Data Flow Control, Message Data Size Control

Description	Short Name	Option Name
MSS(Maximum Segment Size) in the HpFP protocol		hpfp-mss

Data Flow Control, Data Buffer Setting

Description	Short Name	Option Name
Set the sending buffer size for the HpFP protocol		hpfp-sndbuf
Set the receiving buffer size for the HpFP protocol		hpfp-rcvbuf

Authentication

Description	Short Name	Option Name
Specify a username first and ownership change		user
Specify a password first and ownership change		password

Various Monitorings

Description	Short Name	Option Name
Investigation mode starts (deprecated)		investigation

Log Management

Description	Short Name	Option Name
Specify an application diagnostic log output destination		hcp-diag
Specify various statistics log output destinations		stat-log-file
Specify an execution record output destination		<u>hcp-out</u>
Start in the multiple-run mode		multi-run

Software Information Update

Description	Short Name	Option Name
Check the application version	V	<u>version</u>
Check the configuration and input parameters		<u>config-test</u>
Display the command help	h	<u>help</u>

System Operating Environment Settings

Description	Short Name	Option Name
Setting form a path of the configuration file		config-file
Make configuration from command line		config-option
Show configuration option's names		show-config-options
Setting by a relative path from the current directory		include-conf-from-cwd
Server compatibility disabled		no-earlier-serv-compat

Check System Information

Description	Short Name	Option Name
Show system info		system-info
Run host benchmark		run-host-benchmark
Specify measurement categories on the benchmark		run-host-benchmark-categories

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

```
--investigation
```

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

```
--hpfp, --user, --password, --config-file, --config-option, --show-config-options,
--system-info, --run-host-benchmark, --run-host-benchmark-categories, --hcp-diag, -
-stat-log-file, --udp, --hpfp-cong, --hpfp-mss, --hpfp-sndbuf, --hpfp-rcvbuf, --mul
ti-run, --include-conf-from-cwd, --no-earlier-serv-compat, --no-agent, --ident-sele
ct
```

6.10.3 Ownership Change

6.10.3.1 d, no-dereference

```
=====
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 ...
--
```

6.10.3.2 R, recursive

```
=====
Format : -R | --recursive
=====
```

Changes owner or group of files traversing directories recursively.

Ownerships and groups of all subdirectories under the specified directory will be changed.

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

6.10.3.3 s, follow-cmd-link-dir

```
=====  
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.

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

6.10.3.4 S, follow-all

```
=====  
Format : -S | --follow-all  
=====
```

Change owner or group of files following all symbolic links to directories.

```
--  
Example:  
[user@localhost ~]$ hchown -S ...  
--
```

6.10.3.5 D, no-follow

```
=====  
Format : -D | --no-follow  
=====
```

Change owner or group of files without following symbolic links to directories.

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

6.10.3.6 host

```
=====
Format : --host=<remote-host>
-----
remote-host
Default : none
Range of Values : IP address or host name
=====
```

The remote host in the destination is specified. This option is applied to a link target or link name, or a path to specify a directory. With this parameter, the host name for this path can be omitted.

```
--
Example:
[user@localhost ~]$ hchown --remote-host=192.168.100.100 ...
--
```

6.10.3.7 port

```
=====
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. This option is applied to a link target or link name, or a path to specify a directory.

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

6.10.4 Log Management

6.10.4.1 hcp-out

```
=====
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=- ...
TODO
EXIT 0 REASON 0000
[user@localhost ~]$
--

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

6.10.5 Software Information Update

6.10.5.1 V, version

```
=====
Format : -V | --version
=====
```

The hchown command version is shown.

```
--
Example:
[user@localhost ~]$ hchown -V
```

```
hchown client (hchown) 1.5.17_27 / Linux (HpFP2 2.0.0.91_40 WSAPI 0.0.1.36 WS 4.2.0
-2)
--
```

6.10.5.2 config-test

```
=====
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 ~/.ssh/id_ed25
519 ~/.hcp/id_rsa ~/.hcp/id_ecdsa ~/.hcp/id_ed25519]
MaxReceiveRate            : 1000000000000
```

```

MaxSendRate           : 100000000000
MaxConnectionReceiveRate : 100000000000
MaxConnectionSendRate  : 100000000000
TransportTimeout       : 180 sec
AcceptableCryptMethod  : AES256/GCM AES256/CTR/VMAC AES256/CBC AES128/CB
C [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.
--

```

6.10.5.3 h, help

```

=====
Format : -h | --help
=====

```

The hchown command help is shown.

```

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

```

6.11 Command Execution Mode

NEC Ultra-high-speed Data Transfer System 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.

6.11.1 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)  
[user@localhost ~]$ hcp src.txt dest.txt  
...  
[user@localhost ~]$ echo $?  
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)
```

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)  
.hcp.statistics.transport.tcp (Linux)  
.hcp.statistics.transport.hpfp (Linux)
```

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
--
```

6.11.2 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.
2019/11/01 14:04:23 00007fb04eac3b80:      :Logging on multi-running is configured (ID=hcp.mr.20191101_140423_458.15318, dir=/var/tmp, path=/var/tmp/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 unlimited since the specified value is over 5Gbps (given limit : 10000000000 bps).
```

```

2019/11/01 14:04:23 00007fb04eac3b80:INFO :Set bandwidth inbound to unlimited since
the specified value is over 5Gbps (given limit : 10000000000 bps).
2019/11/01 14:04:26 00007fb04736a700:INFO :A transport timeout monitor was setup (s
ock=6, _recv). Monitoring the timeout ...

[user@localhost ~]$ cat /var/tmp/hcp.mr.20191101_140423_458.15318.out | grep -e EXI
T
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 out - put 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.hpfp
```

7 Client Configuration

7.1 Client Setting Files

7.1.1 The Kinds and Reading Order of the Setting Files

NEC Ultra-high-speed Data Transfer System provides the following configuration files on the client.

command name	file name
hcp	hcp.conf
hsync	hsync.conf
hrm	hrm.conf
hcp-ls	hcp-ls.conf
hmkdir	hmkdir.conf
hpwd	hpwd.conf
hmv	hmv.conf
hln	hln.conf
hchmod	hchmod.conf
hchown	hchown.conf

Each command load the following configuration files in the order. 'hcp.conf' is an example representation to describe the order.

1. /etc/hcp/hcp.conf (Linux)
2. <user home directory>/.hcp/hcp.conf (Linux)
3. <the path configured in the `config-file` 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.

You need a privilege to edit /etc/hcp/hcp.conf in the first file of No.1.

If you change configurations in ordinary users, please use the second file of <user home directory>/.hcp/hcp.conf or the third file of <the path configured in the `config-file` options>.

7.1.2 Including Setting Files

On each configuration file, You can load an external configuration file, noted as 'common configuration file' below, to share the configuration across any client configuration files. This results in preventing you from writing a configuration to each configuration file respectively and saving time to change your configuration.

1. Create a common configuration file to describe configurations to share across client configuration files. For example, the file name is 'hcp-common.conf' here.

2. Add an including statement to hcp.conf.

```
[root@localhost ~]# vi hcp.conf Include /etc/hcp/hcp-common.conf // Specifying a common configuration file in an absolute path or relative one.
```

3. Add the including statements to other client configuration files of hsync.conf, hrm.conf, hcp-ls.conf, hmkdir.conf, hpwd.conf, hmv.conf, hln.conf, hchmod.conf, hchown.conf in the same manner.

And you can write this including statement in any place on the configuration files. Loaded configurations from the statement overwrites configurations loaded before. You cannot make nesting the including statement.

When you specify the common configuration file in a relative path, NEC Ultra-high-speed Data Transfer System searches for it in relative from client configuration files to include it.

7.2 Client Common Command Setting Items

7.2.1 Setting Item List

The setting items for the common settings with the client commands are below.

System Operating Environment Settings, Transmission Method Related

Description	Configuration Name
Protocol version (fixed to 2)	ProtocolVersion

Communication Data Compression Function

Description	Configuration Name
Compress level	<u>CompressLevel</u>
Header compression	<u>HeaderCompress</u>
Content compression	<u>ContentCompress</u>

Data Flow Control, Bandwidth Control

Description	Configuration Name
Max receiving rate (per session)	<u>MaxReceiveRate</u>
Max sending rate (per session)	<u>MaxSendRate</u>
Max receive rate (per connection)	<u>MaxConnectionReceiveRate</u>
Max send rate (per connection)	<u>MaxConnectionSendRate</u>

Data Flow Control, File Lock Function

Description	Configuration Name
Use file lock	<u>FileLock</u>
Number of trials to lock files	<u>FileLockTrials</u>
The trial interval (in seconds)	<u>FileLockTrialInterval</u>

Data Flow Control, Data Buffer Setting

Description	Configuration Name
Maximum buffer allocation size	<u>MaxBufferSize</u>
HpFP transport buffer size extension	<u>UDPTransportExtensionBufferSize</u>
TCP sending buffer	<u>TCPTransportSocketSendBuffer</u>

Data Flow Control, Transfer File Size Control

Description	Configuration Name
Maximum receiving file size	<u>MaxReceiveFileSize</u>
Maximum sending file size	<u>MaxSendFileSize</u>

Data Flow Control, Message Data Size Control

Description	Configuration Name
Initial header block size	<u>InitHeaderBlockSize</u>
Initial content block size	<u>InitContentBlockSize</u>
Maximum header block size	<u>MaxHeaderBlockSize</u>
Maximum content block size	<u>MaxContentBlockSize</u>
Max file entry request	<u>MaxRequestFileEntryAtOnce</u>

Code Transformation, Communication Encoding Negotiation

Description	Configuration Name
Transport character encoding	<u>TransportCharEncoding</u>

Code Transformation, Host Character Encoding

Description	Configuration Name
Host character encoding	<u>HostEncoding</u>

Authentication

Description	Configuration Name
PAM (Pluggable Authentication Module) authentication	<u>PAMAuthentication</u>
Public key authentication	<u>PubkeyAuthentication</u>
Number of prompts to enter password	<u>NumberOfPasswordPrompts</u>
Specify directory for searching private keys (RSA auth)	<u>IdentitySearchDir</u>
Specify file for finding a private key (RSA auth)	<u>IdentityFile</u>
Configure priority of public key authentication	<u>PubkeyAuthenticationPrior</u>

Encryption

Description	Configuration Name
Encryption method for message communication	<u>AcceptableCryptMethod</u>
Digest method for validation of message and file data	<u>AcceptableDigestMethod</u>
Disable MAC (Message Authentication Code) or not	<u>DisableDataIntegrityChecking</u>
Acceptance of rejection for disabling MAC	<u>AcceptDataIntegrityCheckingOnRejection</u>

Security Negotiation by Encryption Communications

Description	Configuration Name
Server host key's acceptance policy configuration	<u>StrictHostKeyChecking</u>

Various Monitoring, Timeout Control

Description	Configuration Name
Set transport timeout	<u>TransportTimeout</u>

Performance Evaluation

Description	Configuration Name
How to make pre-allocation in disk benchmark	<u>DiskBenchmarkPreAllocation</u>
A unit size for the pre-allocation	<u>DiskBenchmarkPreAllocationSize</u>
Direct I/O benchmark, alignment size specification	<u>DiskBenchmarkDirectAlignmentSize</u>
Async I/O benchmark, NO_WAIT(reserved)	<u>DiskBenchmarkAsyncNoWait</u>
Async I/O benchmark, maximum number of I/O events at once	<u>DiskBenchmarkAsyncMaxEvents</u>
Async I/O benchmark, maximum number of taking event results at once	<u>DiskBenchmarkAsyncMaxGetEvents</u>
Async I/O benchmark, a size of pool holding request buffers	<u>DiskBenchmarkAsyncRequestPoolSize</u>
File size on additional disk benchmarks	<u>DeepDiskBenchmarkFileSize</u>
Required free space on the benchmarks	<u>DeepDiskBenchmarkFreeSpaceRequired</u>
A set of block sizes on the benchmarks	<u>DeepDiskBenchmarkBlockSizes</u>

Log Management

Description	Configuration Name
Application diagnostic log configuration (ApplicationLog as old one)	<u>DiagnosticLog</u>
Application diagnostic log level (ApplicationLogLevel as old one)	<u>DiagnosticLogLevel</u>
Application statistics configuration	<u>ApplicationStatLog</u>
Transport statistics configuration	<u>TransportStatLog</u>
Set to output a security detail on application statistics	<u>ApplicationStatLogSecurityEx</u>

System Operating Environment Settings, CPU Thread Control

Description	Configuration Name
Limit number of threads to use (Linux)	<u>MaxConcurrentThread</u>

7.2.2 System Operating Environment Settings, Transmission Method Related

7.2.3 Communication Data Compression Function

7.2.3.1 CompressLevel

```
=====
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.

7.2.3.2 HeaderCompress

```
=====
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
--
```

7.2.3.3 ContentCompress

```
=====
Format : ContentCompress <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

The compression of the data of files, data blocks created from the files, is configured.

```
--
Example :
ContentCompress no
--
```

7.2.4 Data Flow Control, Bandwidth Control

7.2.4.1 MaxReceiveRate

```
=====
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
--
```

7.2.4.2 MaxSendRate

```
=====
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
--
```

7.2.4.3 MaxConnectionReceiveRate

```
=====
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
--
```

7.2.4.4 MaxConnectionSendRate

```
=====
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
--
```

7.2.5 Data Flow Control, File Lock Function

7.2.5.1 FileLock

Refer to the hcpd configurations.

7.2.5.2 FileLockTrials

Refer to the hcpd configurations.

7.2.5.3 FileLockTrialInterval

Refer to the hcpd configurations.

7.2.6 Data Flow Control, Data Buffer Setting

7.2.6.1 MaxBufferSize

```
=====
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
--
```

7.2.6.2 UDPTransportExtensionBufferSize

```
=====
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
--
```

7.2.6.3 TCPTransportSocketSendBuffer

```
=====
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  
--
```

7.2.7 Data Flow Control, Transfer File Size Control

7.2.7.1 MaxReceiveFileSize

```
=====  
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  
--
```

7.2.7.2 MaxSendFileSize

```
=====  
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
--
```

7.2.8 Data Flow Control, Message Data Size Control

7.2.8.1 InitHeaderBlockSize

```
=====
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.

7.2.8.2 InitContentBlockSize

```
=====
Format : InitContentBlockSize <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.

7.2.8.3 MaxHeaderBlockSize

```
=====
Format : MaxHeaderBlockSize <block-size>
-----
block-size
Default : 50KB
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.

7.2.8.4 MaxContentSize

```
=====
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.

7.2.8.5 MaxRequestFileEntryAtOnce

```
=====  
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  
--
```

7.2.9 Code Transformation, Communication Encoding Negotiation

7.2.9.1 TransportCharEncoding

```
=====  
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.

7.2.10 Code Transformation, Host Character Encoding

7.2.10.1 HostEncoding

```
=====
Format : HostEncoding <encoding>
-----
encoding
Default :
  UTF-8 (Linux)
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
--
```

7.2.11 Authentication

7.2.11.1 PAMAuthentication

```
=====  
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  
--
```

7.2.11.2 PubkeyAuthentication

```
=====  
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  
--
```

7.2.11.3 NumberOfPasswordPrompts

```
=====
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 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
--
```

7.2.11.4 IdentitySearchDir

```
=====
Format : IdentitySearchDir <flag-available>
-----
flag-available
Default :
    /etc/hcp/keys (Linux)
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.

This software supports the following formats of private keys.

- PEM
- OpenSSH v1
- PuTTY v2/v3

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.

The old name of 'PrivateKeySearchDir' is available.

7.2.11.5 IdentityFile

```
=====
Format : IdentityFile <file-path>
-----
file-path
Default :
(Linux)
~/.ssh/id_rsa ~/.ssh/id_ecdsa ~/.ssh/id_ed25519
~/.hpc/id_rsa ~/.hpc/id_ecdsa ~/.hpc/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.

This software supports the following formats of private keys.

- PEM
- OpenSSH v1
- PuTTY v2/v3

About key algorithms, the following algorithms are supported.

- RSA (1024bits - 4096bits)
- ECDSA nistp256, nistp384, nistp521
- Ed25519

TOKENS of %, %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.

The old name of 'PrivateKeyFile' is available.

7.2.11.6 PubkeyAuthenticationPrior

```
=====
Format : PubkeyAuthenticationPrior <flag-available>
-----
flag-available
Default : yes
Range of Values : yes, no
=====
```

Whether 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. 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
--
```

7.2.12 Encryption

7.2.12.1 AcceptableCryptMethod

```
=====
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/HMAC,
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 the server. The algorithm is chosen to match the server configuration.

7.2.12.2 AcceptableDigestMethod

```
=====
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 for data communication and verification of transferred files 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.

7.2.12.3 DisableDataIntegrityChecking

```
=====
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  
--
```

7.2.12.4 AcceptDataIntegrityCheckingOnRejection

```
=====  
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  
--
```

7.2.13 Security Negotiation by Encryption Communications

7.2.13.1 StrictHostKeyChecking

```
=====
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
--
```

7.2.14 Various Monitoring, Timeout Control

7.2.14.1 TransportTimeout

Refer to the hcpd configurations.

7.2.15 Performance Evaluation

7.2.15.1 DiskBenchmarkPreAllocation

```
=====
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  
--
```

7.2.15.2 DiskBenchmarkPreAllocationSize

```
=====  
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 benchmark (one time allocation).

```
--  
Example :  
DiskBenchmarkPreAllocationSize 1GB  
--
```

7.2.15.3 DiskBenchmarkDirectAlignmentSize

```
=====
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
--
```

7.2.15.4 DiskBenchmarkAsyncNoWait (reserved)

7.2.15.5 DiskBenchmarkAsyncMaxEvents

```
=====
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
--
```

7.2.15.6 DiskBenchmarkAsyncMaxGetEvents

```
=====
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
--
```

7.2.15.7 DiskBenchmarkAsyncRequestPoolSize

```
=====
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
--
```

7.2.15.8 DeepDiskBenchmarkFileSize

```
=====
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
--
```

7.2.15.9 DeepDiskBenchmarkFreeSpaceRequired

```
=====
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
--
```

7.2.15.10 DeepDiskBenchmarkBlockSizes

```
=====  
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  
--
```

7.2.16 Log Management

7.2.16.1 DiagnosticLog

```
=====  
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  
-----  
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 application diagnostic log settings. The log includes some details of errors for trouble shooting.

log-level specifies the log level.

With flag-available yes, the log is output.

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.

log-path specifies the log path. When it is set with the command line parameter "-l" simultaneously, the command line parameter setting is applied.

```

--
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.

7.2.16.2 DiagnosticLogLevel

```

=====
Format : DiagnosticLogLevel <log-level>
-----
log-level

```

```
Default : INFO
Range of Values : EMERG, ALERT, CRIT, ERR, WARNING, INFO, DEBUG
=====
```

The application diagnostic 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.

7.2.16.3 ApplicationStatLog

```
=====
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
--
```

7.2.16.4 TransportStatLog

```
=====
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 “DatePattern” as each criterion, the rotations are carried out as below.

```
// FileSize cases
<specified path>.transport.tcp
<specified path>.transport.tcp.1
<specified path>.transport.tcp.2
...
<specified path>.transport.tcp.n
// DatePattern cases
<specified path>.transport.tcp
<specified path>.transport.tcp.2019-12-10
<specified path>.transport.tcp.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
--
```

7.2.16.5 ApplicationStatLogSecurityEx

```
=====
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
--
```

7.2.17 System Operating Environment Settings, CPU Thread Control

7.2.17.1 MaxConcurrentThread

```
=====
Format : MaxConcurrentThread <max-threads>
-----
max-threads
Default : 0
Range of Values : signed integer
=====
```

The maximum number of threads is configured.

7.3 Client Command Setting Items (hcp)

7.3.1 Setting Item List

The setting items for the hcp commands are below. (Except for the common settings with the client commands)

Data Flow Control, Temporary File Save Function (Atomic File Save)

Description	Configuration Name
Atomically file saving	<u>AtomicLikeSaving</u>
Threshold for atomically file saving	<u>AtomicLikeSavingThreshold</u>

Data Flow Control, Disk I/O Speed Control

Description	Configuration Name
Disk I/O reading rate per session	<u>MaxReadRate</u>
Disk I/O writing rate per session	<u>MaxWriteRate</u>

Retransmission Function

Description	Configuration Name
Number of auto resuming trials	<u>AutoResumeTrials</u>
Interval time between trials (in seconds)	<u>AutoResumeTrialInterval</u>

Performance Evaluation

Description	Configuration Name
Memory copy parallelism (when disabling local disk I/O)	<u>MemoryTransferConcurrency</u>

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>
cp/synchronizationn setting	<u>UseProperCopyAndSync</u>

7.3.2 Data Flow Control, Temporary File Save Function (Atomic File Save)

7.3.2.1 AtomicLikeSaving

Refer to the hcpd configurations.

7.3.2.2 AtomicLikeSavingThreshold

Refer to the hcpd configurations.

7.3.3 Data Flow Control, Disk I/O Speed Control

7.3.3.1 MaxReadRate

```
=====
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  
--
```

7.3.3.2 MaxWriteRate

```
=====  
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  
--
```

7.3.4 Retransmission Function

7.3.4.1 AutoResumeTrials

```
=====  
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  
--
```

7.3.4.2 AutoResumeTrialInterval

```
=====  
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  
--
```

7.3.5 Performance Evaluation

7.3.5.1 MemoryTransferConcurrency

```
=====  
Format : MemoryTransferConcurrency <num-concur> <wait-type> <busy-sleep-nsec>  
-----  
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 se
conds
--
```

7.3.6 System Operating Environment Settings

7.3.6.1 Include

```
=====
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 overwitten.“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.

7.3.6.2 UseProperCopyAndSync

```
=====
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).
- ㄠ 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 --

7.4 Client Command Setting Items (hsync)

7.4.1 Setting Item List

The setting items for the hsync commands are below. (Except for the common settings with the client commands)

Retransmission Function

Description	Configuration Name
Number of auto rerun trials	<u>AutoRerunTrials</u>
Interval time between trials (in seconds)	<u>AutoRerunTrialInterval</u>

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.4.2 Retransmission Function

7.4.2.1 AutoRerunTrials

```
=====
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
--
```

7.4.2.2 AutoRerunTrialInterval

```
=====
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
--
```

7.4.3 System Operating Environment Settings

7.4.3.1 Include

Refer to the hcp command configurations.

7.5 Client Command Setting Items (hrm)

7.5.1 Setting Item List

The setting items for the hrm commands are below. (Except for the common settings with the client commands)

Description	Configuration Name
Including setting files	<u>Include</u>

7.5.2 System Operating Environment Settings

7.5.2.1 Include

Refer to the hcp command configurations.

7.6 Client Command Setting Items (hcp-ls)

7.6.1 Setting Item List

The setting items for the hcp-ls commands are below. (Except for the common settings with the client commands)

Description	Configuration Name
Including setting files	<u>Include</u>

7.6.2 System Operating Environment Settings

7.6.2.1 Include

Refer to the hcp command configurations.

7.7 Client Command Setting Items (hmkdir)

7.7.1 Setting Item List

The setting items for the hmkdir commands are below. (Except for the common settings with the client commands)

Description	Configuration Name
Including setting files	<u>Include</u>

7.7.2 System Operating Environment Settings

7.7.2.1 Include

Refer to the hcp command configurations.

7.8 Client Command Setting Items (hpwd)

7.8.1 Setting Item List

The setting items for the hpwd commands are below. (Except for the common settings with the client commands)

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.8.2 System Operating Environment Settings

7.8.2.1 Include

Refer to the hcp command configurations.

7.9 Client Command Setting Items (hmv)

7.9.1 Setting Item List

The setting items for the hmv commands are below. (Except for the common settings with the client commands)

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.9.2 System Operating Environment Settings

7.9.2.1 Include

Refer to the hcp command configurations.

7.10 Client Command Setting Items (hln)

7.10.1 Setting Item List

The setting items for the hln commands are below. (Except for the common settings with the client commands)

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.10.2 System Operating Environment Settings

7.10.2.1 Include

Refer to the hcp command configurations.

7.11 Client Command Setting Items (hchmod)

7.11.1 Setting Item List

The setting items for the hchmod commands are below. (Except for the common settings with the client commands)

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.11.2 System Operating Environment Settings

7.11.2.1 Include

Refer to the hcp command configurations.

7.12 Client Command Setting Items (hchown)

7.12.1 Setting Item List

The setting items for the hchown commands are below. (Except for the common settings with the client commands)

System Operating Environment Settings

Description	Configuration Name
Including setting files	<u>Include</u>

7.12.2 System Operating Environment Settings

7.12.2.1 Include

Refer to the hcp command configurations.

8 Error Codes and Signals

8.1 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_FAILURE	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

8.2 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 : PPubkeyAuthenti  
cation 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

8.3 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

Reason code (Hexadecimal)	name	description
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
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

Reason code (Hexadecimal)	name	description
A019	CANNOT_WRITE_DANGLING_SYM LINK	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
FFFF	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
BFF2	SCH_BIND_CANCELED	secondary channel binding canceled
BFF3	SCH_ALREADY_SHUTDOWN	secondary channel 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

8.4 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
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
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
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
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.

8.5 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.

9 Statictics Information

9.1 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	Description
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
```

The file process reason code 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

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.

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], 85
90723508, 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), 192.16
8.30.51:35880, 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], 21
60, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC], None, HpFP [N / MSS145
6], 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], 21
60, 0, 1, 0, 0.000000, UTF8, AES/CTR/NoPadding SHA256 [MAC / B128 K256 VmacAES], No
ne, 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], 24
80, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA25
6], 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], 24
80, 0, 1, 0, 0.000000, UTF8, AES/CBC/PKCS5Padding SHA256 [MAC / B128 K256 HmacSHA25
6], 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 [PKA], hcp (t
x) [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 [PKA], hcp (t
x) [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 [PKA], hcp (t
x) [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 [PAM], hcp (t
x) [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 [PAM], 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 [PAM], 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 [PAM], 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
--

```

9.2 Transport Statistics

9.2.1 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)
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.aaaaaa (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, 6712.942871, 516
3.802246, 6712.854004, 5163.731934
2018/05/25 15:05:53.321617, 4436, 2920, 4436, 2920, 654830, 12764, 0, 78369.882812,
51587.031250, 16918.314453, 11775.388672
--
```

9.2.2 HpFP Statistics

During HpFP communicating, The traffic and transport statistics are recorded periodically (approximately every 1 second) on the server and client.

Column 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)
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 (b
ps), TpRx (bps), AvgTpTx (bps), AvgTpRx (bps)
2019/10/30 09:34:17.520056, 0, 0, 0, 0, 89560, 382, 0, 0, 1236, 0, 0, 0.000000, 0.0
00000, 0.000000, 0.000000
2019/10/30 09:34:19.915566, 1052, 1124, 1052, 66536, 89560, 382, 0, 0, 1236, 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
--
```

9.3 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 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)
Sess	The number of incoming sessions
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
WorkSess	The number of processing sessions
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 sessions which has been connected before this record is logged is recorded in Sess (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 sessions at the time is recorded in WorkSess (present value).

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), Sess, Conn, TCPConn,  
HpFPConn, HTTPConn, UserConn, WorkSess, WorkConn, WorkTCPConn, WorkHpFPConn, Work  
kHTTPConn  
2025/01/10 14:52:07.682780, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0  
2025/01/10 14:52:17.784830, 29768, 6847, 29768, 660515, 1, 5, 5, 0, 0, 1, 1, 5, 5,  
0, 0  
2025/01/10 14:52:27.872202, 15260, 12852, 15260, 12852, 0, 0, 0, 0, 0, 0, 1, 5, 5,  
0, 0  
--
```

A Appendix

A.1 Notes

A.1.1 Common considerations on performance characteristics

Application performance can be affected by the following factors.

- File Size

Transferring a large number of small files tends to cause a drop in throughput.

- Encryption, Compression or Digest Calculation

During transferring, the throughput may decrease due to an increasing load on CPU by a bottleneck of encryption or decryption processing.

And it also can decrease during encryption processing if AES-NI acceleration is unavailable.

In networks over 1 Gbps, cipher methods, including CBC mode or HMAC digest, may cause a bottleneck in cryptographic processing even though AES-NI is functional, which could result in throughput drops.

- Block Size

When transferring files in bandwidth over 10Gbps utilizing the multi-channel function, the following parameters should be set from 1MB to 4MB.

- InitContentBlockSize
- MaxContentBlockSize

When the parameters are set around 100KB, the performance may not be reached the expected level (approximately from 60Gbps to 70Gbps on TCP multi-channel) due to the burden of the synchronization process - ing to bond channels for multiplexing.

When using encryption and setting this parameter over 1MB, its performance might meet a decrease because of data transfer between AES-NI module's buffer and system memory (load of cache in-out). Please try again setting a parameter less than current one you set.

- Number of Connections in Multi-Channel

A number of connections from 8 to 16 is optimal for the multi-channel function. When the number is over the range, the performance tends to decrease due to overhead processing many connections.

- Usage on Wide band Disk I/O (Linux)

When a limited disk I/O performance appears with disks having I/O performance from 40Gbps to 100Gbps in a normal usage of reading and writing files, using options of Direct I/O or asynchronous I/O might improve the I/O performance.

When you don't make the performance of 100Gbps in the default configuration using the asynchronous I/O, please try to use `--fio-direct-reuse-aligned` that enables caching buffers for Direct I/O to reuse them and reduce loads of memory allocation or change a value of `--fio-async-max-events` to a larger one.

- Memory Usage Limitation

`MaxTotalBufferSize` might cause a performance bottleneck in simultaneous multiple connections in broadband environments. Because the buffer is shared with these multiple sessions.

- Log Level or Debug Log

When the log level gets `DEBUG` in the following, or debug log gets enabled, the performance might decrease.

Configuration File or Command	Setting Item or Option Name
hcpd.conf	SystemLogLevel and set it to <code>DEBUG</code>
hcp.conf or other client configuration files	DiagnosticLogLevel and set it to <code>DEBUG</code>
All commands	<code>--investigation</code> option and use it

A.1.2 Considerations on performance characteristics (HpFP)

Transport performance would be affected by the following factors.

- MTU Size

When MTU size is about 1.5KB, HpFP throughput may not be able to achieve 10Gbps. Jumbo frame, whose MTU is about 9KB, is recommended in the environment over several Gbps.

- IP Network Buffer Size

When the following OS's parameters are small, HpFP might not be able to achieve around 10Gbps throughput due to packet loss.

- `net.core.rmem_max`
- `net.core.wmem_max`

- CPU Power Saving Mode

CPU performance may get lower than required for high bandwidth transport by the following OS power-saving configuration, which may degrade HpFP performance.

- Linux

`/sys/devices/system/cpu/cpu*/cpufreq/scaling_governor`

- Packet Queue Size on Intermediate Network Equipment

When the network includes devices with small queue sizes or equivalent conditions, packet loss may happen without RTT increase, where HpFP can't properly work the congestion control function and cause decreases in the performance or fairness.

- Congestion Control Mode

The aggressive mode of HpFP is an experimental function. In the mode, the performance may decrease because of packet loss under situations with high processing load like transmitting over 10Gbps. Especially, when using the multi-channel function, the throughput might be unstable due to uneven distribution of processing on CPUs that would be driven by the RSS (Receive Side Scaling) function of NIC (Network Interface Card). In these cases, the Fair mode is recommended.

A.1.3 Considerations Regarding Features

- When Using the Same UDP Port to Plural hcpd Processes

When connecting from a client using `UDPListenAddress(deprecated,)` problems, such as a connection timeout, etc., might happen and not work as expected. `HPFPListenAdr` doesn't cause.

Example :

```
--
hcpd1
UDPListenAddress 0.0.0.0:884
* The UDP port number 65520 is used as default. The privileged port number is 884
.

systemctl start hcpd
* Start hcpd as daemon.
--

--
hcpd2
UDPListenAddress 0.0.0.0:1884
* The UDP port number 65520 is used as default. The non-privileged port number is
1884.
```

```
hcpd -f -c ~/hcpd.conf -p ~/hcpd.pid
* Start hcpd in foreground.
--
```

This configuration result in using the same UDP port of 65520 on two hcpd processes while service ports of 884 and 1884 are different.

The following is the command to connect from a client to a host running in the above configuration.

```
--
hcp --udp=D:D:D:D:D my_src.txt 192.168.100.100:884:my_dst.txt
--
```

This would, however, result in server connection timeout.

Workaround: Change the UDP port number for one of the hcpd processes as below.

```
UDPListenAddress 0.0.0.0:1884:65519
```

- Workaround for the Issue That a Process is Killed by Linux OOM (Out Of Memory) Killer

As an OS mechanism, Linux monitors memory consumption for each process and terminates the processes running out of memory.

If the following buffer size is set to larger than the system memory, Linux OOM Killer might kill the process.

Configuration File	Setting Item
hcp.conf	MaxBufferSize
hcpd.conf	MaxTotalBufferSize

Workaround: Lower the buffer size or increase the system memory.

- Log Level or Debug Log

When the log level gets DEBUG in the following, or debug log gets enabled, a timeout might happen because transmitting files take a long time, which has been found in environments via NAT.

Configuration File or Command	Setting Item or Option Name
hcpd.conf	SystemLogLevel and set it to DEBUG
hcp.conf or other client configuration files	DiagnosticLogLevel and set it to DEBUG
All commands	--investigation option and use it

A.2 NEC Ultra-high-speed Data Transfer System 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 characters of 1 line in users	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 incompatible characters, newline code and so on
The number of file cache entries	100000entries
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

A.3 Trademarks

Company names, product names, and service names used in this document are trademarks or registered trademarks of their respective owners.

- NEC and NEC product names are trademarks or registered trademarks of NEC Corporation.
- Red Hat and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc.
- Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Trademark symbols (™, ®, etc.) are omitted in this document.

A.4 Revision History

Revision	Publication Date	Changes
2nd Edition	July 27, 2026	Version 1.0.1 supported
1st Edition	January 20, 2026	Version 1.0 supported

A.5 Document Information

- **Document Title:** NEC Ultra-high-speed Data Transfer System Manual
- **Applicable Version:** 1.0.1
- **Edition:** 2nd Edition
- **Publication Date:** July 27, 2026
- **Publisher:** NEC Corporation

Copyright 2022 CLEALINK TECHNOLOGY Co., Ltd.
Modified and published by NEC Corporation.