English

Fujitsu Software BS2000

CLIP V21.0B10

Common Logging Interface Provider

User Guide

June 2025

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to: bs2000services@fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2015

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2015.

Copyright and Trademarks

Table of Contents

CLIP

1 Preface

CLIP is a BS2000 software product designed to integrate BS2000-specific messages, security-related information, and events, and to centrally forward them to an external security management system, such as a SIEM system.

In the BS2000 operating system, messages and events from various components such as the Security Audit Trail log (SATLOG file), ACCOUNTING, console logging (CONSLOG file), and software error logging (SERSLOG file), are recorded in separate log files.

CLIP is designed to collect various events within the BS2000 system and convert them into the format defined by the Syslog protocol (RFC 5424). These messages are sent via socket connections to an external server that supports the Syslog format, such as a Linux-based rSyslog server. The external server can collect, filter, and process events from multiple BS2000 systems, which can then be analyzed and visualized by a SIEM system.

CLIP currently supports BS2000 events and messages from the following components:

- Events logged by SAT (Security Audit Trail), which are recorded in the BS2000 SAT log file (SATLOG) and can be analyzed using the SATUT utility.
- ACCOUNTING entries for resource usage billing.

1.1 Target audience

The "Clip User Guide" is intended for BS2000 system administrators and elevated users who operate the CLIP subsystem and rsyslog server administrators on LINUX machines that configure rsyslog.

A comprehensive understanding of BS2000 and LINUX operating systems is necessary to operate CLIP.

1.2 Summary of content

This manual describes the basic structure, functions, and usage of the CLIP subsystem.

The chapter **"**Software product CLIP**"** provides an overview of the structure, installation, and configuration of the CLIP product.

The chapters **"**CLIP-Architecture**"** and **"**Syslog protocol**"** explain the architecture and supported formats used by CLIP.

At the end of the manual, you will find various examples to help you work more easily with this documentation.

1.3 Changes since the last edition

Changes in CLIP v21.0B10

- In the parameter file a filter for SATLOG events can now be configured
- CLIP has been extended by the ACCOUNTING record types

Changes in CLIP v21.0B01

- IPv6 and FQDN are now supported
- In Parameter file parameter "LOGSERVER" may be used interchangeable with "IP"
- SATCP extended logging is supported

1.4 Notational conventions

The following typographical elements are used in this manual:

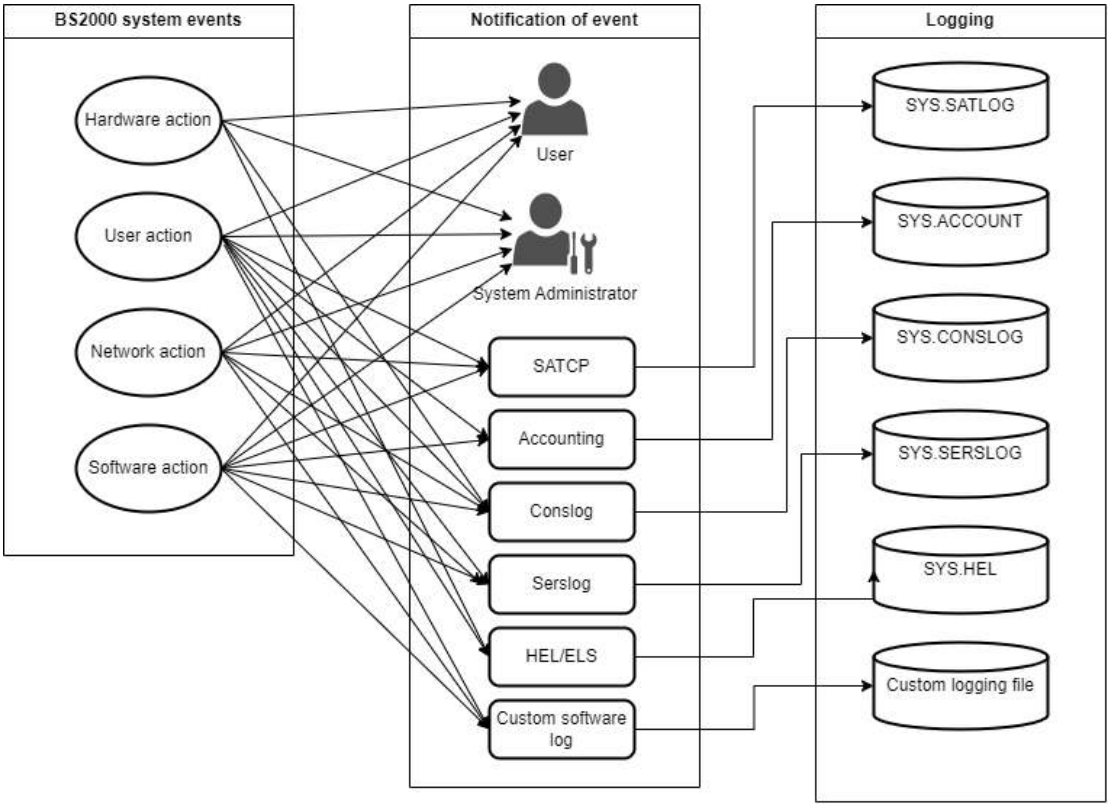
`INPUT`	Inputs in examples are shown in bold typewriter font
`Output`	Outputs in examples are shown in typewriter font

2 Logging in the BS2000 system

In the BS2000 operating system, as in any other operating system, it is ensured that system administration is informed of all relevant events. Such events may be triggered by hardware and/or software, as well as by user actions or automated processes.

All of these events are logged within the system by different components and in various files. In BS2000, examples include SAT, ACCOUNTING, and CONSLOG. Depending on the logging component, events are therefore recorded in different formats, for instance, in a binary format for SAT, or in a printable message format for CONSLOG.

The diagram below illustrates the typical flow of information logging that are relevant for evaluation in the BS2000 operating system.



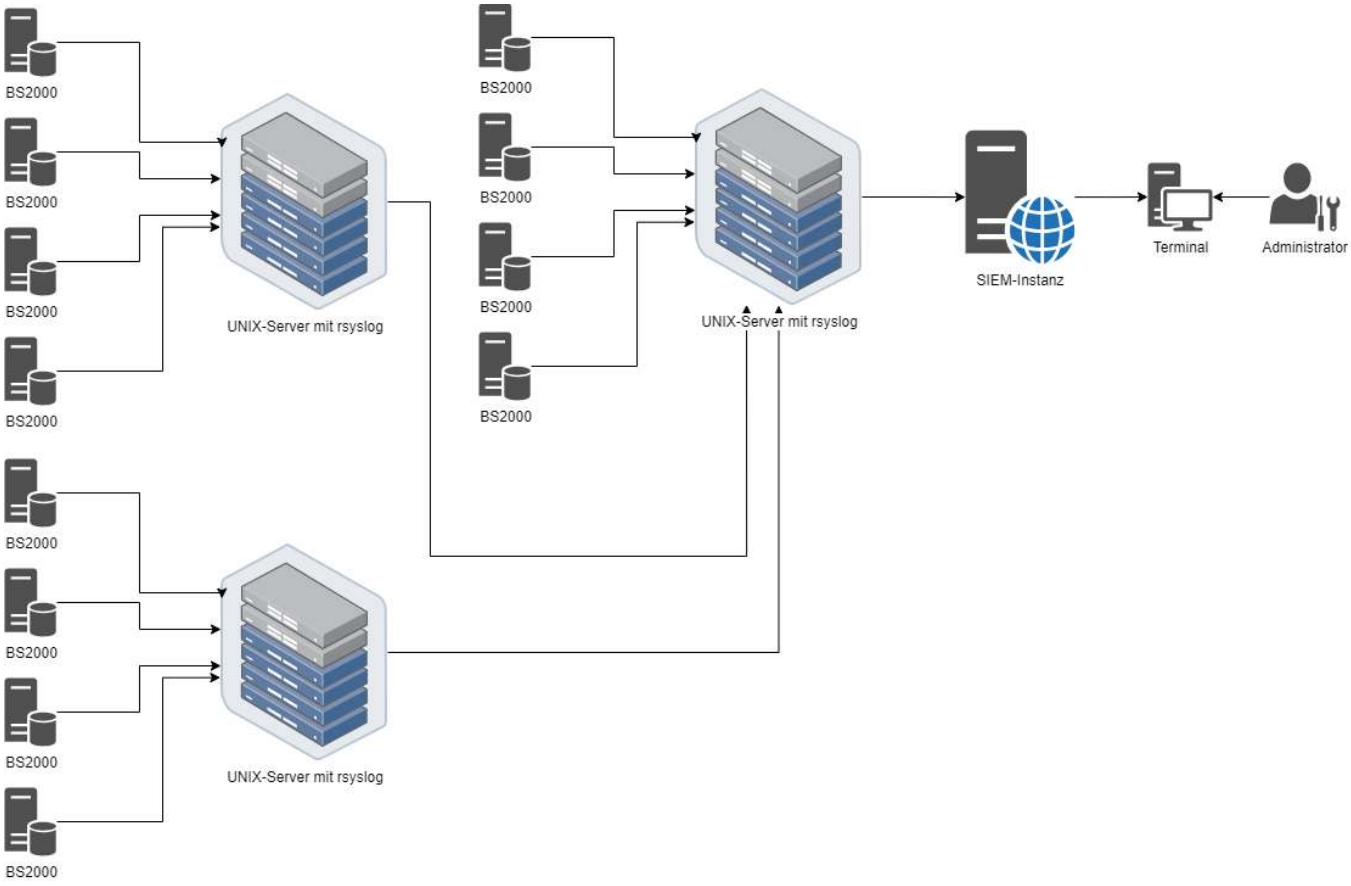
The quantity of events produced by an operating system during operation may be substantial. Therefore, filtration and pre-selection methods are utilized in specific logging tools and are documented in the BS2000 documentation.

The CLIP subsystem in BS2000 provides a unified interface that collects security-relevant BS2000 messages and events produced by different components, maps them to the standardized Syslog protocol format and forwards them to an external server, such as an rSyslog server, for further processing. From there, they can be routed to a central SIEM system for analysis.

In the current version of CLIP, the following BS2000 events are supported and made available for external analysis:

- SAT (Security Audit Trail)
- ACCOUNTING (Accounting Records)

In the example scenario shown below, rSyslog servers are used to illustrate the setup. These servers receive and store events from multiple BS2000 systems. The rSyslog servers themselves can also be cascaded, meaning they can forward the received events to a central rSyslog server, which aggregates all events. This central server can then pass the data on to a SIEM instance for further analysis. The scenario demonstrates the scalability of the infrastructure.



3 Syslog protocol

The original syslog protocol was defined in RFC 3164. However, since it was never officially standardized, a new standard, RFC 5424, was introduced to clarify and extend the specification. CLIP transmits messages exclusively in the RFC 5424 format. Configuration is done using the parameters facility: 1 (user-level messages) and severity: 6 (informational).

Field names and values are represented as `"field"="value"` pairs, separated by spaces.

The different value types are formatted and transmitted in ASCII as follows:

- c-strings remain unchanged
- Numbers are represented as strings of digits (0–9)
- x-strings are represented as strings of hexadecimal characters (0–9, A–F)
- Keywords are translated into their corresponding descriptive meanings

Currently, CLIP processes security-relevant BS2000 events and messages from the following sources and forwards them in RFC 5424-compliant syslog format to an external server, such as an rSyslog server:

- **SAT (Security Audit Trail)**
  Field names and values are documented in the official SECOS manual.

  > **Note**
  > HEADER and TRAILER record of a SAT file are written directly to the file. Therefore, the corresponding SAT events ZBG and ZND are not transferred to CLIP and cannot be logged there.

- **ACCOUNTING (Accounting records)**
  Details are provided in the following section.

rSyslog is a widely used open-source tool for forwarding log messages based on the syslog protocol.

The message format used by CLIP is described below. The structure of the header fields is defined in RFC 5424.

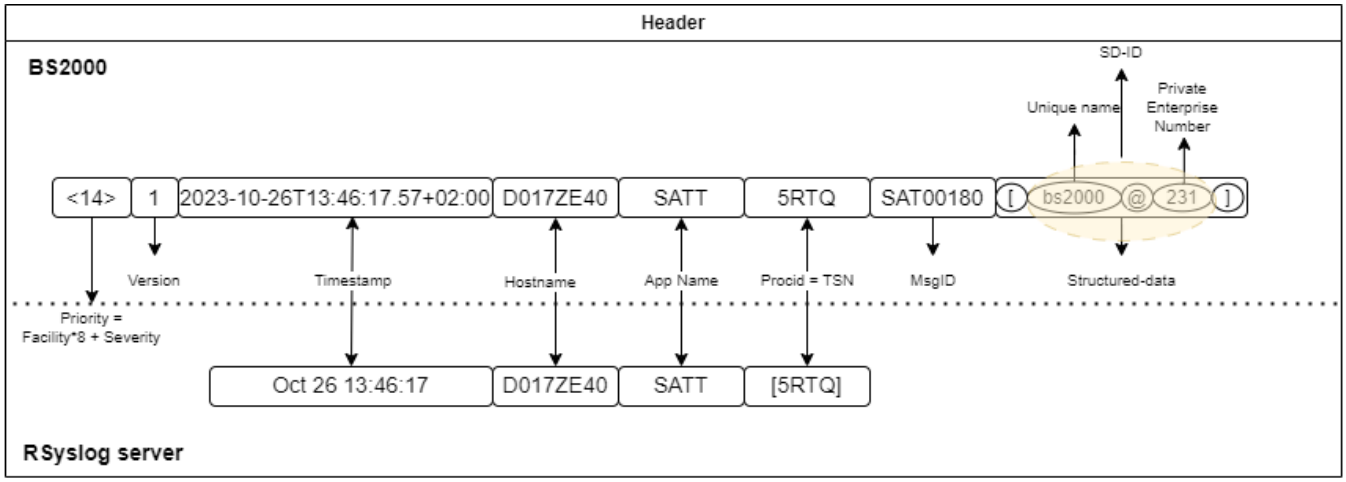
Example of a syslog message transmitted by CLIP over the network interface:

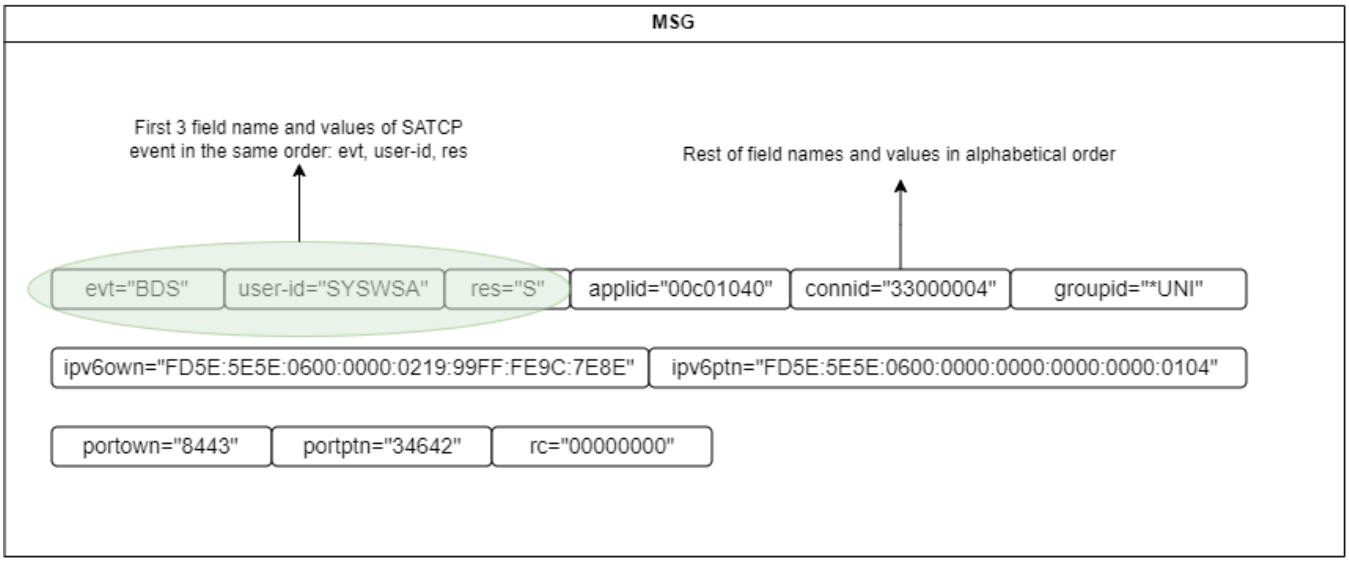
```
<14>1 2023-10-26T13:46:17.57+02:00 D017ZE40 SATT 5RTQ SAT00180 [bs2000@231] evt="
BDS" user-id="SYSWSA" res="S" applid="00c01040" connid="33000004" groupid="*UNI"
ipv6own="FD5E:5E5E:0600:0000:0219:99FF:FE9C:7E8E" ipv6ptn="FD5E:5E5E:0600:0000:0000:
0000:0000:0104" portown="8443" portptn="34642" rc="00000000"
```

Example of how this message is displayed on a Linux rSyslog server:

```
Oct 26 13:46:17 D017ZE40 SATT[5RTQ] evt="BDS" user-id="SYSWSA" res="S" applid="
00c01040" connid="33000004" groupid="*UNI" ipv6own="FD5E:5E5E:0600:0000:0219:99FF:
FE9C:7E8E" ipv6ptn="FD5E:5E5E:0600:0000:0000:0000:0000:0104" portown="8443" portptn="
34642" rc="00000000"
```

The structure of the message is illustrated in the figures that follow.


Header
BS2000
SD-ID
Unique name
Private Enterprise Number
<14>
1
2023-10-26T13:46:17.57+02:00
D017ZE40
SATT
5RTQ
SAT00180
[
bs2000
@
231
]
Version
Timestamp
Hostname
App Name
Procid = TSN
MsgID
Structured-data
Priority = Facility*8 + Severity
Oct 26 13:46:17
D017ZE40
SATT
[5RTQ]
RSyslog server


MSG
First 3 field name and values of SATCP event in the same order: evt, user-id, res
Rest of field names and values in alphabetical order
evt="BDS"
user-id="SYSWSA"
res="S"
applid="00c01040"
connid="33000004"
groupid="*UNI"
ipv6own="FD5E:5E5E:0600:0000:0219:99FF:FE9C:7E8E"
ipv6ptn="FD5E:5E5E:0600:0000:0000:0000:0000:0104"
portown="8443"
portptn="34642"
rc="00000000"

3.1 Accounting-Logs

In the table below the individual fields from the ACCOUNTING record types are defined in detail. For further information, please refer to the "Accounting records" manual as well as the relevant specific manuals (see also the overview of accounting records in "Introduction to System Administration").

The following applies for field names that are listed with an <x>:

For some accounting records a prefix consisting of 2 letters and a suffix consisting of an ascending number with 2 digits is appended to the field name.
Example: Field 1 is listed as "userid<x>". Both accounting records DSPC and DSPP use this field variably, which is why a prefix and a suffix is appended for these accounting records. Thus, the complete field names for those two accounting records are as follows:

For DSPC: SPuserid01, SPuserid02, SPuserid03, ...
For DSPP: PSuserid01, PSuserid02, PSuserid03, ...

All remaining accounting records use the static name, therefore the field for the accounting record "JOBS" is named: userid

Field ID	Field name	Field description	Possible accounting logs containing this field
1	userid<x>	User ID	JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS<COx>, DSPC<SPx>, DSPP<PSx>, DRFA, FTR0, SOPA
2	accnr<x>	Account number	JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS<COx>, DRFA, FTR0, SOPA
3	tsn<x>	TSN	JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS<COx>, DRFA, FTR0, SOPA
4	group	Group name	JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS, DRFA, FTR0, SOPA
5	ident	Pubset identifier "PUB"	DSPC, DALC
6	catid	Catalog ID	DSPC, DALC, AOPN, ACLS
7	ownerid	Owner ID	DSPC, DALC
8	vsn	VSN of the disk	DSPP, DRVR
9	mnemonic	Mnemonic name of the disk	DSPP
10	install	Installation designation	AOPN, ACLS
11	osname	Operating system name	AOPN, ACLS
12	osver	Operating system version	AOPN, ACLS

13	session	Session number	AOPN, ACLS
14	maxcpu	'E' if more than 8 CPU-IDs	AOPN, ACLS
15	install2	Installation identifier	AOPN, ACLS
16	intface	Hardware and software interface	AOPN, ACLS
17	cpuid1	CPU-IDs 1-8	AOPN, ACLS
18	cpuid2	CPU-IDs 9-16	AOPN, ACLS
19	extvers	Extended version identifier	AOPN, ACLS
23	subname	Name of the subsystem	ESMC, ESMD
24	subvers	Subsystem version	ESMC, ESMD
25	calldat	Date of call	ESMC, ESMD
26	calltim	Time of call	ESMC, ESMD
27	jobacdat	Date of job acceptance	JOBS
28	jobactim	Time of job acceptance	JOBS
29	jobstdat	Date of job start	JOBS, TASK, PRGS, PRGT, PACC, UACC
30	jobsttim	Time of job start	JOBS, TASK, PRGS, PRGT, PACC, UACC
31	jobname	Job name	JOBS, SPLI
32	jobaccen	Century of job acceptance	JOBS
33	jobstcen	Century of job start	JOBS, TASK, PRGS, PRGT, PACC, UACC
34	jobacsea	Season identifier of job acceptance	JOBS
35	jobstsea	Season identifier of job start	JOBS, TASK, PRGS, PRGT, PACC, UACC
36	tsktmdat	Date of task termination	TASK
37	tsktmtim	Time of task termination	TASK
38	tskcpu	Task CPU time	TASK, PRGS, PRGT, PACC, UACC, HSMS, RCPU, SOPA
39	inoutnr<x>	Number of inputs /outputs	TASK, PRGS, PRGT, PACC, UACC, HSMS, TDEV<DUx, DVx, VUx>, SOPA
40	dattrans<x>	Volume of data transferred	TASK, PRGS, PRGT, PACC, UACC, TDEV<DUx, DVx, VUx>

41	mainmem	Main memory allocation integral	TASK, PRGS, PRGT, PACC, UACC
42	resmem	Resident memory pool integral	TASK, PRGS, PRGT, PACC, UACC
43	pagingnr	Number of paging operations	TASK, PRGS, PRGT, PACC, UACC
44	tskprio	Task scheduling priority	JOBS, TASK, PRGS, PRGT, PACC, UACC
45	tskatt	Task scheduling attribute	JOBS, TASK, PRGS, PRGT, PACC, UACC
46	secmoutm	SECURE and MOUNT waiting time	TASK, PRGS, PRGT, PACC, UACC
47	tsktype	Task category	JOBS, TASK, PRGS, PRGT, PACC, UACC
48	jobtmcen	Century of job termination	TASK
49	vecpages	Vector pages integral	TASK, PRGS, PRGT, PACC, UACC
50	resspace	Resident DATA SPACE integral	TASK, PRGS, PRGT, PACC, UACC
51	jobtmsea	Season identifier of job termination	TASK
52	stdcpu	Standardized CPU time	TASK, PRGS, PRGT, PACC, UACC
53	390mode	390 mode time	TASK, PRGS, PRGT, PACC, UACC
54	prgstdat	Date of program start	PRGS
55	prgsttim	Time of program start	PRGS
56	prgstcen	Century of program start	PRGS
57	prgstsea	Season identifier of program start	PRGS
58	prgtmdat	Date of program termination	PRGT
59	prgtmtim	Time of program termination	PRGT
60	prgtmcen	Century of program termination	PRGT
61	prgtmsea	Season identifier of program termination	PRGT

62	recdat	Date of recording	PACC, UACC, RCPU
63	rectim	Time of recording	PACC, UACC, RCPU
64	reccen	Century of recording	PACC
65	recsea	Season identifier for writing this record	PACC
66	dumpsdat	Date of dump start	PDMP
67	dumpstim	Time of dump start	PDMP
68	dumpedat	Date of dump end	PDMP
69	dumpetim	Time of dump end	PDMP
70	dumppag	Number of main memory pages output	PDMP
71	dumptsk	TSN of dump task	PDMP
72	crashtsk	TSN of affected task	PDMP
73	splosdat	Date of spoolout start	SPLO
74	splostim	Time of spoolout start	SPLO
75	sploedat	Date of spoolout end	SPLO
76	sploetim	Time of spoolout end	SPLO
77	splonam	Spoolout job name	SPLO
78	copycnt	Number of copies to be output	SPLO
79	splocls	Spoolout class	SPLO
80	sploprio	Spoolout scheduling priority	SPLO
81	splotype	Type of spoolout file	SPLO
82	sploscen	Century for spoolout	SPLO
83	splossea	Season identifier for spoolout start	SPLO
84	sploesea	Season identifier for spoolout end	SPLO
85	sploecen	Century for spoolout end	SPLO

86	prnttsn	TSN of the partner print job	SPLO
87	reldat	Date of release	TDEV
88	reltim	Time of release	TDEV
89	relcen	Century of release	TDEV
90	relsea	Season identifier for release	TDEV
91	tskmddat	Date of task modification	TATR
92	tskmdtim	Time of task modification	TATR
93	tskmdpri	New task scheduling priority	TATR
94	tskmdatt	New task scheduling attribute	TATR
95	tskmdcen	Century of task modification	TATR
96	tskmdsea	Season identifier for task modification	TATR
97	stktime	Date and time of stocktaking	DSPC, DSPP
98	compstat	Completeness indicator	DSPC
99	curcen	Current century	UACC, DSPC, DALC, DSPP, RCPU
100	cursea	Season identifier for current time	UACC, DSPC, DSPP, ESMC, ESMD, RCPU
101	recavdat	Date of record availability	DALC
102	udatdat	Date of invocation	UDAT
103	udatim	Time of invocation	UDAT
104	udatcen	Century of invocation	UDAT
105	udatsea	Season identifier for invocation	UDAT
106	sysidat	Date of system initialization	AOPN
107	sysitim	Time of system initialization	AOPN
108	filodat	Date of file opening	AOPN

109	filotim	Time of file opening	AOPN
110	filorea	Cause of file opening	AOPN
111	sysicen	Century of system initialization	AOPN
112	filocen	Century of file opening	AOPN
113	sysisea	Season identifier for system initialization	AOPN
114	filosea	Season identifier for file opening	AOPN
115	timezon	Time zone	AOPN
116	timediff	Time difference	AOPN
117	filcdat	Date of file closure	ACLS
118	filctim	Time of file closure	ACLS
119	filcrea	Cause of file closure	ACLS
120	filccen	Century of file closure	ACLS
121	filcsea	Season identifier for file closure	ACLS
122	intcpu	Interrupt analysis CPU time	RCPU
123	idlecpu	CPU idle time	RCPU
124	spoolid	"SPOOLOUT"	RSRV
125	spooldev	Type of spoolout device	RSRV
126	spoolmne	Mnemonic name of spoolout device	RSRV
127	spooltsn	TSN of spoolout driver task	RSRV
128	substati	Subsystem status flag (initialization)	ESMC
129	substatt	Subsystem status flag (termination)	ESMD
256	extid1	Extension identifier 1	JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, DSPC, DSPP, DALC, UDAT, UACC, AOPN, ACLS, RSRV, HSMS, BCA4, SPLI, SRBS, VACD, DRFA, FTR0
257	extid2	Extension identifier 2	JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, AOPN, ACLS, RSRV, HSMS, BCA4, SPLI, FTR0

258	extid3	Extension identifier 3	JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, AOPN, HSMS, BCA4, FTR0
259	extid4	Extension identifier 4	JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, FTR0
260	extid5	Extension identifier 5	TASK, PRGS, PRGT, PACC, SPLO, UACC
261	extid6	Extension identifier 6	TASK, PRGS, PRGT, PACC, SPLO, UACC
262	extid7	Extension identifier 7	TASK, PRGS, PRGT, PACC, SPLO
263	extid8	Extension identifier 8	PRGT
264	extid9	Extension identifier 9	-
266	extcase	Extension case identifier	JOBS, SPLO, RSRV
272	joborig	Place of job creation	JOBS
273	jobcrea	Job creator	JOBS
274	jservnam	Name of server where the job was created	JOBS
275	jcreatsn	TSN of creator job	JOBS, SPLO
276	diatype	Type of dialog partner	JOBS
277	servnam	Server name	JOBS
278	termapp	Name of terminal or application	JOBS
279	termtyp	Terminal type	JOBS
280	repcnt	Repetition counter	JOBS
281	subsid	Identifier of the subsystem that created the subjob	JOBS
282	jobclass	Job class	JOBS
283	jobprio	Job scheduling priority	JOBS
284	jobsinf	Job start information	JOBS
285	cputimel	Specified CPU time limit	JOBS
286	printlim	Specified PRINT limit	JOBS

287	punchlim	Specified PUNCH limit	JOBS
288	jobpar	Job parameter	JOBS
289	termrea<x>	Termination indication	TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx>
290	termunit	Termination unit	TASK, PRGT
291	termorig<x>	Termination request	TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx>
292	termcode<x>	Termination code	TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx>
293	cl56mem	Total class 5 and 6 memory allocation	TASK, PRGS, PRGT, PACC, UACC
294	commem	Common memory pool integral	TASK, PRGS, PRGT, PACC, UACC
295	eammem	EAM memory allocation	TASK, PRGS, PRGT, PACC, UACC
296	datspace	DATA-SPACE integral	TASK, PRGS, PRGT, PACC, UACC
297	iopubvol	Number of I/Os for public volume sets	TASK, PRGS, PRGT, PACC, UACC, HSMS
298	ioshprv	Number of I/Os for shareable private disks	TASK, PRGS, PRGT, PACC, UACC, HSMS
299	ioexprv	Number of I/Os for exclusive private disks	TASK, PRGS, PRGT, PACC, UACC, HSMS
300	iomtape	Number of I/Os for magnetic tapes	TASK, PRGS, PRGT, PACC, UACC, HSMS
301	iorecdev	Number of I/Os for unit-record devices	TASK, PRGS, PRGT, PACC, UACC, HSMS
302	dtpubvol	Data transferred for public volume sets	TASK, PRGS, PRGT, PACC, UACC
303	dtshprv	Data transferred for shareable private disks	TASK, PRGS, PRGT, PACC, UACC
304	dtexprv	Data transferred for exclusive private disks	TASK, PRGS, PRGT, PACC, UACC
305	dtmtape	Data transferred for magnetic tapes	TASK, PRGS, PRGT, PACC, UACC
306	dtrecdev	Data transferred for unit-record devices	TASK, PRGS, PRGT, PACC, UACC
307	iotermlo	Number of terminal I/Os (low)	TASK, PRGS, PRGT, PACC, UACC

308	dttermlo	Number of bytes transferred to/from terminal (low)	TASK, PRGS, PRGT, PACC, UACC
309	iotermhi	Number of terminal I /Os (high)	TASK, PRGS, PRGT, PACC, UACC
310	dttermhi	Number of bytes transferred to/from terminal (high)	TASK, PRGS, PRGT, PACC, UACC
311	locfiacc	Number of catalog accesses to local files	TASK, PRGS, PRGT, PACC, UACC
312	locjvacc	Number of catalog accesses to local job variables	TASK, PRGS, PRGT, PACC, UACC
313	remfiacc	Number of catalog accesses to remote files	TASK, PRGS, PRGT, PACC, UACC
314	remjvacc	Number of catalog accesses to remote job variables	TASK, PRGS, PRGT, PACC, UACC
315	dynserrq	Maximum dynamic SERVICE-RATE request	TASK, PRGS, PRGT, PACC, UACC
316	spservlo	Specified SERVICE-UNITS (low)	TASK, PRGS, PRGT, PACC, UACC
317	spcpulo	Specified CPU-SU (low)	TASK, PRGS, PRGT, PACC, UACC
318	spiolo	Specified IO-SU (low)	TASK, PRGS, PRGT, PACC, UACC
319	spmemlo	Specified MEMORY-SU (low)	TASK, PRGS, PRGT, PACC, UACC
320	spservhi	Specified SERVICE-UNITS (high)	TASK, PRGS, PRGT, PACC, UACC
321	spcpuhi	Specified CPU-SU (high)	TASK, PRGS, PRGT, PACC, UACC
322	spiohi	Specified IO-SU (high)	TASK, PRGS, PRGT, PACC, UACC
323	spmemhi	Specified MEMORY-SU (high)	TASK, PRGS, PRGT, PACC, UACC
324	stdcpusu	Standardized CPU-SU	TASK, PRGS, PRGT, PACC, UACC
325	stdservu	Standardized SERVICE UNITS	TASK, PRGS, PRGT, PACC, UACC
326	accid	Account ID	TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, HSMS

327	progorig	Program origin indicator	PRGS
328	resrea	Restart indicator	PRGS
329	proginf	Additional info to program origin	PRGS
330	prgversh	Program version (10 characters)	PRGS
331	prgname	Program or module name	PRGS
332	prgvercp	Program version (complete)	PRGS
333	filenam	File name	PRGT
334	elemnam	Element name	PRGT, SPLO
335	elemver	Element version	PRGT, SPLO
336	elemtyp	Element type	PRGT, SPLO
337	prevdat	Date of previous PACC log	PACC
338	prevtim	Time of previous PACC log	PACC
339	prevcen	Century of previous PACC log	PACC
340	prevsea	Season identifier of previous PACC log	PACC
341	splocrea	Date and time of spoolout job creation	SPLO
342	origuser	Original user ID (for spoolout)	SPLO
343	tapedev	Mnemonic name of tape device	SPLO
344	printdev	Mnemonic name of printer	SPLO
345	linecnt	Number of printed lines	SPLO, RSRV, SRBS
346	pagecnt	Number of printed pages	SPLO
347	devname	Device name	SPLO
348	formname	FORM name	SPLO
349	compid	Component identifier	SPLO

350	devmnem<x>	Mnemonic device name	SPLO, TDEV<DUx, DVx>, VACD
351	devacc	Device Access	SPLO
352	#pdsxmit	# of xmits for the pds	SPLO
353	#prntpag	# of printed pages-side	SPLO
354	#timeseg	Time used (.01 sec)	SPLO
355	#pagedef	Number of requested PAGEDEF	SPLO
356	#formdef	Number of requested FORMDEF	SPLO
357	#fontsrq	Number of requested FONTS	SPLO
358	#fontsld	Number of FONTS loaded	SPLO
359	#overlrq	Number of requested overlays	SPLO
360	#overlld	Number of overlays loaded	SPLO
361	#pagused	Size of pages used	SPLO
362	flginp	Input bin flag	SPLO
363	flgout	Output bin flag	SPLO
364	flgdup	Duplex flag	SPLO
365	splofil	Name of spoolout file	SPLO
366	reccnt	Number of records	SPLO
367	devtype<x>	Device type	TDEV<DUx, DVx, VUx>, VACD, SPLI
368	occtime<x>	Date and time of start of allocation	TDEV<DUx, DVx, VUx>
369	alloctyp<x>	Allocation type	TDEV<DUx, DVx, VUx>
370	alloccen<x>	Century of allocation start	TDEV<DUx, DVx, VUx>
371	allocsea<x>	Season identifier for allocation start	TDEV<DUx, DVx, VUx>
372	volser#<x>	Volume serial number	TDEV<VUx>

373	rdwrind<x>	Read Write indicator (U/R/W)	TDEV<VUx>
374	pams0occ<x>	Number of occupied PAM blocks level S0	DSPC<SPx>
375	pams1occ<x>	Number of occupied PAM blocks level S1	DSPC<SPx>
376	pams2occ<x>	Number of occupied PAM blocks level S2	DSPC<SPx>
377	occpag#<x>	Number of occupied pages	DSPP<PSx>
378	catfil#<x>	Number of catalogued files	DSPP<PSx>
379	mduserid<x>	Affected user ID	DALC<ALx>
380	pamoccto<x>	Number of occupied PAM blocks	DALC<ALx>
381	spacemdv<x>	Space modification value	DALC<ALx>
382	reqtsn<x>	TSN of requesting task	DALC<ALx>
383	moddate<x>	Date of modification	DALC<ALx>
384	modtime<x>	Time of modification	DALC<ALx>
385	spacetyp<x>	Space type	DALC<ALx>
386	sysid<x>	System ID	DALC<ALx>
387	modsea<x>	Season identifier of modification	DALC<ALx>
388	userdat	User data	UDAT
389	pfilenam	Name of preceding file	AOPN
390	mainmems	Main memory size	AOPN
391	pagemems	Size of pageable memory	AOPN
392	sysspadd	Beginning of system address space	AOPN
393	sysspsz	Size of system address space	AOPN
394	cpuidx	CPU-IDs 17-X	AOPN, ACLS

395	sfilenam	Name of successor file	ACLS
396	splocnt	Number of spoolout processes	RSRV, SRBS
397	bytecnt	Number of printed bytes	RSRV, SRBS
398	servsdat	Date of service task start	RSRV
399	servstim	Time of service task start	RSRV
400	servedat	Date of service task end	RSRV
401	servetim	Time of service task end	RSRV
402	ordrtime	Timestamp of the order	HSMS
403	taskid	Identifier of the task type	HSMS
404	tsnrun	TSN of the running task	HSMS
405	recindex	Record index	HSMS, SOPA
406	accnrlen<x>	Length of the accounting number of batch orders	HSMS<COx>
407	accnr<x>	Accounting number of batch orders	HSMS<COx>
408	ownproc	Own processor name	BCA4
409	ownappl	Own application name	BCA4
410	ownproc#	Own processor number	BCA4
411	ownreg	Own region number	BCA4
412	ownlan	Own LAN address	BCA4
512	vmindex	VM index	VACD, VACM
513	vmname	VM name	VACD, VACM
514	vmreldat	Date of release of devices	VACD
515	vmreltim	Time of release of devices	VACD

516	vmrelcen	Century of release of devices	VACD
517	vmrelsea	Season identifier for release of devices	VACD
518	vmedat	Date of VM stop	VACM
519	vmetim	Time of VM stop	VACM
520	vmsdat	Date of VM start	VACM
521	vmstim	Time of VM start	VACM
522	usecpus	Consumed CPU time in seconds	VACM
523	usecpums	Consumed CPU time in microseconds	VACM
524	memsizmb	Memory size in MB	VACM
525	strsizmb	Expanded storage size in MB	VACM
526	vmecen	Century of VM stop	VACM
527	vmscen	Century of VM start	VACM
528	vmesea	Season identifier of VM stop	VACM
529	vmssea	Season identifier of VM start	VACM
530	rescpus	CPU reserved time in seconds	VACM
531	rescpums	CPU reserved time in microseconds	VACM
532	memsizho	Memory size in high order bytes	VACM
533	strsizho	Expanded storage size in high order bytes	VACM
534	utmapp	Application name of UTM application	UTMA, UTMK
535	utmuser	Name of the UTM user	UTMA, UTMK
536	signtim	Sign-on time	UTMA
537	utmtime	Date and time of record creation	UTMA

538	utmaccnt	Accounting unit counter	UTMA
539	utmtacnt	Number of TACs called with TACUNIT > 0	UTMA
540	utmtrans	Transaction code of the program unit	UTMK
541	utmcpu	CPU time in openUTM in msec	UTMK
542	dtsyscpu	CPU time in the database system in msec	UTMK
543	utmio	Number of IOs in openUTM	UTMK
544	dtsysio	Number of IOs in the database system	UTMK
545	msinlen	Length of the input message	UTMK
546	msoutlen	Length of the output message	UTMK
547	asynout	Number of asynchronous outputs	UTMK
548	accltac	Accounting units for LTACs	UTMK
549	ltermnam	Name of the LTERM partner	UTMK
550	progrtim	Real time of the program unit run in msec	UTMK
551	mnemfir	Mnemonic of the first device	DRVR
552	mnemsec	Mnemonic of the second device	DRVR
553	evtype	Type of event	DRVR
554	spacetim	Timestamp of SPACEOPT	SOPA
555	rfasdat	Date of RFA connection set	DRFA
556	rfastim	Time of RFA connection set	DRFA

557	rfaedat	Date of RFA session end	DRFA
558	rfaetim	Time of RFA session end	DRFA
559	afrcatid	Catalogue ID of partner system	DRFA
560	afrproc	MRS-Processor name of partner	DRFA
561	afruid	User ID of AFR partner task	DRFA
562	afraccnr	Account number of AFR partner task	DRFA
563	afrtsn	TSN of AFR partner task	DRFA
564	trarec#	# of transferred records	DRFA
565	trabyte#	# of transferred bytes	DRFA
566	rfascen	Century of RFA connection set	DRFA
567	rfaecen	Century of RFA session end	DRFA
568	trasdat	Date of transfer request	FTR0
569	trastim	Time of transfer request	FTR0
570	traedat	Date of transfer end	FTR0
571	traetim	Time of transfer end	FTR0
572	trares	Transfer result	FTR0
573	folres	Follow up processing result	FTR0
574	partnam	Partner name	FTR0
575	reqorig	Request origin	FTR0
576	reqident	Request identification	FTR0
577	dskacc#	Number of disk accesses	FTR0
578	dskbyte#	Number of bytes on disk	FTR0

579	netbyte#	Number of bytes in network	FTR0
580	splisdat	Date of spoolin start	SPLI
581	splistim	Time of spoolin start	SPLI
582	spliedat	Date of spoolin end	SPLI
583	splietim	Time of spoolin end	SPLI
584	#bsplfil	Number of bytes written to spoolin file	SPLI
585	#bdatfil	Number of bytes written to data files	SPLI
586	sessdat	Date of session start	SRBS
587	sesstim	Time of session start	SRBS
588	sesedat	Date of session end	SRBS
589	sesetim	Time of session end	SRBS
590	rbatstat	Name of remote batch station	SRBS
591	splicnt	Number of spoolin jobs	SRBS
592	consdat	Date of connection	BCA4
593	constim	Time of connection	BCA4
594	conedat	Date of disconnection	BCA4
595	conetim	Time of disconnection	BCA4
596	contim	Connection endurance	BCA4
597	recvbyt#	Number of received bytes	BCA4
598	sendbyt#	Number of sent bytes	BCA4
599	parproc#	Partner processor number	BCA4
600	parreg	Partner region number	BCA4
601	parappl	Partner application name	BCA4
602	parlan	Partner LAN address	BCA4

603	paraddr	Partner internet address	BCA4
604	lparnam	Local name for partner	BCA4
605	rfassea	Season identifier of RFA connection set	DRFA
606	rfaesea	Season identifier of RFA session end	DRFA
672	initproc	Initiator	BCA4
673	profile	Profile	BCA4
674	disact	Action causing discon	BCA4
675	sysrea	System reason	BCA4
676	userrea	User reason	BCA4
677	asgdat	Date of device assignment	VACD
678	asgtim	Time of device assignment	VACD
679	asgcen	Century of device assignment	VACD
680	asgsea	Season of Device Assignment	VACD
681	errorcod<x>	Error code	DRFA<STx>
682	tfilenam	Name of transfered file	FTR0
683	libmemt	Library member Type	FTR0
684	libmemvr	Library member version	FTR0
685	libmemva	Library member variant	FTR0
686	libmemna	Library member name	FTR0
687	#locins	Number of used local instructions	FTR0
688	cenreq	Century of transfer request	FTR0
689	cenend	Century of transfer end	FTR0
690	shortmn	Device mn	SPLI

691	#crin	Number of cards read in	SPLI
692	#brin	Number of bytes read in	SPLI, SRBS
693	#rrin	Number of records read in	SPLI, SRBS
694	fdiskvsn	Floppy disk VSN	SPLI
695	splnrbst	Spool name of RB station	SPLI

4 Software product CLIP

The CLIP software product provides services in BS2000 for integrating security-relevant messages and events from the BS2000 system into a SIEM environment.

CLIP is a loadable subsystem in BS2000, part of the BS2000 OS DX package, and is available on current BS2000 servers.

The subsystem consists of a privileged component (TPR) and a non-privileged component (TU). The TU component is loaded by the Job Management System (JMS) when the subsystem is started, while the TPR component is managed by Dynamic Subsystem Management (DSSM).

To execute the program, a batch task of type TP with the job name CLIP is automatically started under the TSOS user ID. This task runs in the background as a daemon.

Main tasks of the TPR component:

- Preparing the execution of the TU component
- Establishing and managing a FITC connection with the TU component
- Receiving interface calls from privileged tasks and transferring them to non-privileged memory
- Communicating with the operator via console messages

Main tasks of the TU component:

- Communicating with the CLIP subsystem (TPR) and receiving messages transmitted from it
- Parsing and processing the incoming messages
- Forwarding the processed messages to a Syslog server, such as an rSyslog server

> The current required product versions and patch levels necessary for operation can be found in the latest BS2000 OS DX release notice.

4.1 Product structure of CLIP

The software product CLIP consists of the CLIP delivery unit, which contains all necessary components for installation and operation.

The CLIP delivery unit includes the following files:

File	Description
SYSDAT.CLIP.<ver>	Configuration file for CLIP
SYSENT.CLIP.<ver>	ENTER job for the CLIP User Task (used internally by CLIP only)
SYSPRG.CLIP.<ver>	Startup program for CLIP (used internally by CLIP only)
SYSLNK.CLIP.<ver>	Load library for /390 servers
SKMLNK.CLIP.<ver>	Load library for x86 servers
SYSMES.CLIP.<ver>	Message file
SYSSSC.CLIP.<ver>	Subsystem declaration
SYSSII.CLIP.<ver>	Installation information for IMON
SYSSPR.CLIP.<ver>	Compiled SDF-P procedure to start the CLIP TU program (used internally by CLIP only)

4.2 Installing and configuring CLIP

The software product CLIP is installed using the installation monitor IMON. The exact installation procedure is described in the current release notes for BS2000 OS DX.

CLIP is delivered with a configuration file named `SYSDAT.CLIP.<ver>` for configuring CLIP.

Changes to the configuration file only take effect after restarting the CLIP subsystem. The configuration settings are described in the section "Configuring CLIP".

4.2.1 Operational resources

CLIP requires a batch task for operation, which is automatically created under the TSOS identifier when the CLIP subsystem starts.

The batch task is started in the default job class (for batch jobs under the TSOS identifier) without a time limit. The task has the job name CLIP.

4.2.2 Software requirements

The CLIP subsystem requires:

- BS2000 OS DX version 1.0B or higher
- For support of SAT (Security Audit Trail), the SECOS product must be installed and the SAT logging component configured.
- For support of ACCOUNTING data, the BS2000 accounting system must be enabled and configured.

4.2.3 Configuring CLIP

CLIP is delivered with a configuration file named SYSDAT.CLIP.<ver> and installed together with the CLIP subsystem. This file must be adapted to the respective configuration. Changes to the configuration only take effect after restarting the CLIP subsystem.

When the CLIP subsystem is loaded, the configuration file is read and evaluated. If errors are found in the configuration file, the loading process continues and default values are applied.

Exceptions to this are syntactically incorrect IP address entries or unreachable IP addresses. In these cases, meaningful operation of CLIP is not possible, and the subsystem startup is terminated with an error.

- If the IP address is syntactically incorrect, the message GLP1020 is output to the console and the CLIP subsystem is terminated:

```
%  GLP1020 READING IP ADDRESS FROM CONFIG FILE FAILED
```

- If the configured IP address is unreachable, the CLIP subsystem will terminate after a timeout expires.

Original configuration file

The configuration file SYSDAT.CLIP.<ver> is delivered as a template with the following content:

```
************************************************************************
*                                                                      *
* Template file: SYSDAT.CLIP.210                                       *
* This file defines necessary parameters for the operation of          *
* the CLIP subsystem.                                                  *
* Additionally, the events to be forwarded to the syslog server      * 
* can also be configured here.                                         *
* More information about this file can be found in the CLIP manual     *
* "Chapter 3.3.5: Parameter file".                                     *
*                                                                      *
************************************************************************
***MANDATORY CONFIG PARAMETERS***
LOGSERVER xxx.xxx.xxx.xxx
***REST OF CONFIG PARAMETERS***
*PORT 514
*PROTOCOL TCP    ONLY VALID OPTION
*HOSTNAME TESTPROC
*TIMEOUT 30
*OVERFLOW 0
***CONFIGURATION FOR LOGFILTER***
*SATT MODE BLOCK/ACCEPT
*SATT EVENTID FAIL/SUCC/BOTH
***CONFIGURATION FOR ACCOUNTING FILTER***
*ACCT MODE BLOCK/ACCEPT
*ACCT RECORDTYPE
```

Syntax of configuration file:

- Lines beginning with ‘*’ are interpreted as comment lines.
- Some parameters have default values and do not need to be specified. The only mandatory parameter is the server address (LOGSERVER), which must be provided by the system administrator.
- Parameters are interpreted regardless of their order.
- Parameter names and their values are case-insensitive and internally converted to uppercase.
- Related parameters must be specified on the same line, separated by at least one space.

- Anything appearing after the last required parameter on a line, separated by at least one space, is treated as a comment.

> The JSON format for the base parameters of the configuration file is supported one last time for compatibility reasons only.

Description of Base Parameters:

- "LOGSERVER" (mandatory)
  Specifies the syslog server to which messages are sent. The value can be an IPv4/IPv6 address or a Fully Qualified Domain Name (FQDN).
  - IPv4 must follow the format xxx.xxx.xxx.xxx (e.g., 192.168.1.99), where each segment is a number between 0 and 255.
  - IPv6 supports both full and abbreviated notations (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334 and 2001:db8:85a3::8a2e:370:7334).
  - If an invalid value is provided, the CLIP program issues an error message and terminates, since a valid server configuration is required.
- "PORT"
  Specifies the port used for communication with the external Syslog server. This must be a valid open port in the range 1 – 65535 on the Syslog server, enabled for the BS2000 server. The parameter defaults to the standard Syslog port 514 (commented out).
- "PROTOCOL"
  Specifies the data transmission protocol between the BS2000 system and the Syslog server. Currently, only TCP is supported. If an incorrect value is entered or the parameter is omitted, the default value "TCP" applies.
- "HOSTNAME"
  Optional, as CLIP automatically determines it if not specified. This parameter defines the BS2000 system’s name and is used to identify the BS2000 system when sending events to the Syslog server. Alphanumeric characters are supported.
- "TIMEOUT"
  Optional; specifies how long CLIP tries to restore the connection in case of disconnection. The value is given in seconds; the default is 30 seconds. If the connection cannot be restored within this period, the CLIP subsystem terminates and must be restarted manually if needed.
- "OVERFLOW"
  Optional; specifies whether CLIP should discard messages if the buffer fills up during a connection loss. A value of 0 (default) causes the subsystem to terminate in this case. If set to 1, the oldest messages in the buffer are overwritten. In both cases, buffered messages are sent once the connection is restored. Whether the subsystem terminates (and thus messages are lost) depends solely on the TIMEOUT value.

Description of Parameters for Filtering Functions

To improve performance and to supply the SIEM environment only with relevant information from the user's perspective, CLIP offers a filtering function. This filter applies independently to SATLOG and ACCOUNTING events.

Filter Function for SATLOG Events:

- "SATT MODE"
  Configures whether the SATLOG events listed in this configuration file are not ("BLOCK") or only ("ACCEPT") forwarded to the Syslog server. If omitted or an invalid value is entered, for compatibility reasons the default "BLOCK" applies.
  - SATT MODE BLOCK (default): All SATLOG events are forwarded to the rSyslog server. Only the SATLOG events listed in this file are filtered out and not forwarded.
  - SATT MODE ACCEPT: SATLOG events are filtered out and not forwarded, except those explicitly listed in this configuration file, which are forwarded to the rSyslog server.
- "SATT <eventid> <result>"
  Adds the event <eventid> to the list defined by "SATT MODE" depending on the result <result>. The event result is interpreted as success ("SUCC"), failure ("FAIL"), or both ("BOTH"). An overview of the SAT events can be found in the SECOS manual in the section "SAT - Logging and Evaluation of Security-Relevant Events".

Filter Function for ACCOUNTING Events:

- "ACCT MODE"
  Configures whether the ACCOUNTING events listed in this configuration file are not ("BLOCK") or only ("ACCEPT") forwarded to the Syslog server. If omitted or an invalid value is entered, the default "BLOCK" applies.
  - ACCT MODE BLOCK (default): All ACCOUNTING events are forwarded to the rSyslog server. Only the ACCOUNTING events listed in this file are filtered out and not forwarded.
  - ACCT MODE ACCEPT: ACCOUNTING events are filtered out and not forwarded, except those explicitly listed here, which are forwarded.
- "ACCT <recordtype>"
  Adds the accounting record <recordtype> to the list defined by "ACCT MODE". All accounting records of the specified type are considered. All event types are listed in the "Accounting-Logs" section.

Example Configuration for the Filter Function:

```
SATT MODE BLOCK
SATT JED  SUCC
SATT UCK  SUCC
SATT FRS  BOTH
```

In this example, BLOCK mode for SATLOG events is enabled. The three subsequent entries specify SATLOG events to be filtered out and therefore **not** forwarded to the Syslog server:

- The event "JED" is filtered only in case of failure.
- The event "UCK" is also filtered only in case of failure.
- The event "FRS" is filtered in both success and failure cases and therefore never forwarded.
- All other events are forwarded without restriction.

If the mode were switched to ACCEPT (SATT MODE ACCEPT), only the events JED and UCK (in success cases only) and the event FRS (in all cases) would be forwarded; all others would be ignored.

Since no ACCOUNTING events are defined, ACCT MODE BLOCK is set automatically. However, because the block list is empty, no ACCOUNTING records are filtered, and all are forwarded to the Syslog server.

4.3 Starting CLIP

After installing CLIP, the CLIP subsystem can be started using the following command:

```
/START-SUBSYSTEM SUBSYSTEM-NAME=CLIP
```

The subsystem is not started automatically after the SYSTEM READY message. It must be started manually by the system administrator or within the CMDFILE.

A successful start of the CLIP subsystem is only possible under the following conditions:

- All required files are installed.
- The CLIP version is compatible with the BS2000 version.
- The IP address and port of the Syslog server are correctly defined in the configuration file.

A successful startup of the CLIP subsystem is logged on the console with the messages GLPLOAD and ESM0220, and can be verified using the command `/SHOW-SUBSYSTEM SUBSYSTEM-NAME=CLIP.`

Subsystem update during ongoing operation:

In the event of a version change of the CLIP subsystem (e.g., installation and startup of a newer version) during ongoing operation, the following steps are required:

- Hold the subsystem CLIP with the command `/STOP-SUBSYSTEM.`
- Install the new version of CLIP on the system.
- Temporarily hold SAT logging with the command:`/HOLD-SAT-LOGGING`.
- Stop the accounting system with the command `/STOP-ACCOUNTING.`
- Start the CLIP subsystem with the command `/START-SUBSYSTEM.`
- Resume SAT logging with the command `/RESUME-SAT-LOGGING`.
- Start the accounting system with the command `/START-ACCOUNTING`

> The above order must be strictly followed. Otherwise, the start of the CLIP subsystem will be denied with the console message:
>
> `GLP1025 START-SUBSYSTEM CLIP IS CURRENTLY NOT POSSIBLE`

> The message file `SYSMES.CLIP.210` will only be updated after the next system restart.

4.4 Terminating CLIP

The CLIP subsystem can be stopped at any time using the following command:

```
/STOP-SUBSYSTEM SUBSYSTEM-NAME=CLIP
```

DSSM automatically waits until the last call to CLIP has been completed.

The following messages are output to the BS2000 console when the CLIP subsystem is stopped:

```
%4XBN-000.135825  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.1305 SEC, USER ID:
TSOS, TASK ID: 00010080, JOB NAME: CLIP
%DSSM-000.135826  %  ESM0220 FUNCTION 'DELETE' FOR SUBSYSTEM 'CLIP    /V21.0'
COMPLETELY PROCESSED
```

4.5 Diagnostic Tools

CLIP is a dynamically loadable subsystem that is decoupled from BS2000.

The tasks generated by CLIP use the job name `CLIP`.

CLIP reports all warning and error messages to the BS2000 console.

CLIP logging information for both the TPR and TU components (e.g., for diagnosing connection issues to the Syslog server) can be found under the TSOS user ID. Under normal operation, the size of these files should not exceed 100 PAM pages per CLIP session.

In the event of issues related to CLIP, the following documentation should be provided for diagnostic purposes:

- CLIP log files, created anew with each subsystem start:
  - SYSLOG.CLIP.TU.<yyyy-mm-dd.hhmmss> – for the batch job
  - SYSLOG.CLIP.SUBS.<yyyy-mm-dd.hhmmss> – for the CLIP subsystem
- CONSLOG file
- System dump (if applicable)
- Diagnostic data from the Syslog server (if applicable)

5 CLIP-Architecture

CLIP, as a BS2000 subsystem, uses the Syslog protocol to support external systems - such as SIEM solutions - in analyzing, consolidating, and storing events from multiple connected BS2000 systems. For this purpose, the CLIP subsystem must be active and properly configured on each monitored BS2000 system.

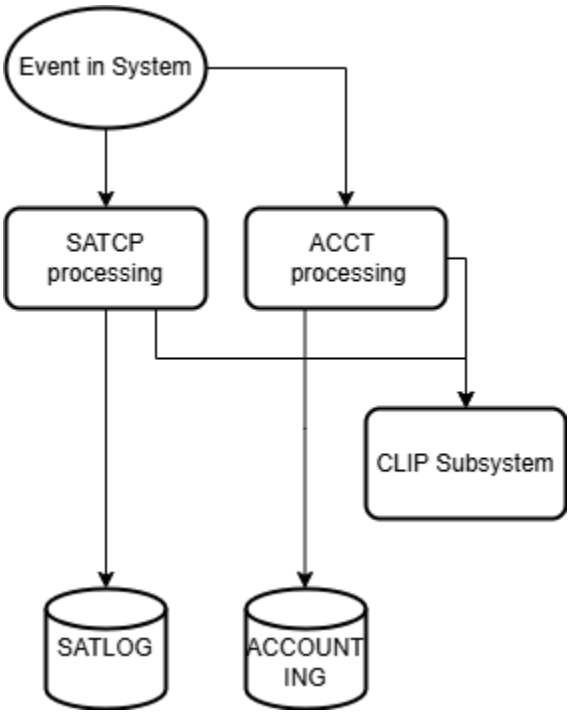
CLIP consists of two components:

- TPR Component: The CLIP subsystem, managed via DSSM, is responsible for central processing of BS2000 events.
- TU Component: A TU batch job that forwards BS2000 events to an external Syslog server using sockets.

TPR Component – CLIP Subsystem

CLIP is provided for the first time starting with BS2000 version V21.0B.

The following diagram illustrates the current CLIP integration with SAT and ACCOUNTING in schematic form.



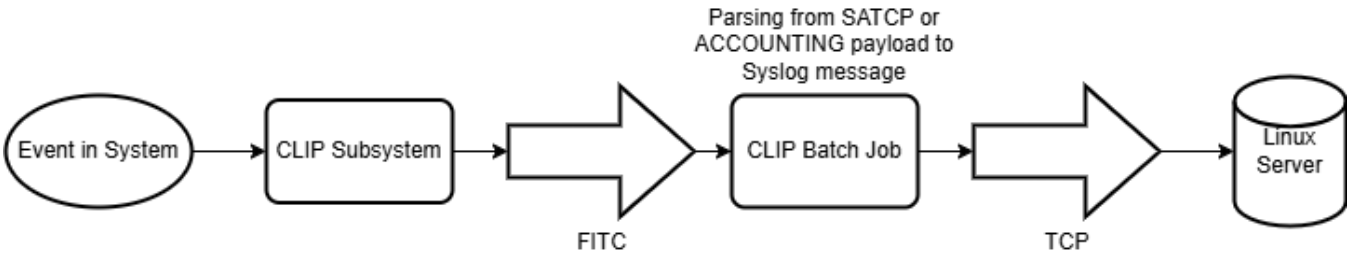
The TPR component of CLIP receives SAT and ACCOUNTING data and passes it on to its TU component.

TU Component – CLIP Batch Job

The CLIP batch job within the TU component establishes a TCP connection to the Syslog server, waits for events from the TPR component, analyzes them, and converts them into the Syslog format. After successful parsing, the events are transmitted via the socket interface to the external server configured in the CLIP configuration file.

A Syslog daemon must be running on the external server on the port configured in CLIP. This daemon receives and filters the incoming data and stores it in the server’s system logs.

The diagram provides a schematic representation of the current CLIP workflow in the TPR and TU components, using SAT and ACCOUNTING as examples.



If the connection to the Syslog server is lost, the batch job will, upon the next event to be sent (occurring at least one second after the connection loss), cyclically attempt to re-establish the connection. This process continues until either a timeout occurs or the internal buffer is full.

6 Example: External Syslog Server – rSyslog

This chapter uses rSyslog as an example of an external Syslog server.

rSyslog is an open-source software tool used on Linux systems to forward log messages over an IP network. It implements the basic Syslog protocol and extends it with content-based filtering and advanced features. The rsyslog service provides capabilities such as filtering, queue management for offline outputs, support for various output modules, flexible configuration options, and the use of TCP for message transport.

rSyslog uses the BSD Syslog standard protocol as defined in RFC 3164. Since RFC 3164 is more of an informational description than a strict standard, several incompatible extensions have been developed. rSyslog supports many of these extensions (including RFC 5424) and allows flexible formatting of forwarded messages (Source: https://en.wikipedia.org/wiki/Rsyslog).

Installation

Install the rSyslog package on an external server or VM (e.g., on an Application Unit (AU)) according to the operating system in use.

Starting the Service

Once installed, you can start/enable the rsyslog.service.

Configuration

Configuration File

The configuration for rSyslog is stored in the file /etc/rsyslog.conf.

To enable reception of CLIP events, the following settings must be added to /etc/rsyslog.conf:

```
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

This activates the TCP input module for the server and opens the default Syslog port (514) to receive incoming messages.

For further configuration options, refer to the official rSyslog documentation.

Facility Level

All messages sent by CLIP are configured in rSyslog with a facility value of 1 (user-level messages) and a severity of 6 (informational).

7 Terminology

ACCOUNTING

System instance for collecting and logging accounting data related to system resources such as CPU time, memory usage, or I/O operations in BS2000.

Batch Job

ENTER job

DSSM (Dynamic Subsystem Management)

DSSM is the central instance in BS2000 for dynamic subsystem management.

ENTER Job

A batch job started BS2000 command sequence (ENTER file).

FQDN (Fully Qualified Domain Name)

Complete domain name.

JMS (Job Management System)

Job control (job management in BS2000).

JSON (JavaScript Object Notation)

File format in readable text form for exchanging structured data between applications.

Linux

Family of multitasking, multiuser operating systems based on the Linux kernel.

Parameter File

Also configuration file. This is a file ($TSOS.SYSDAT.CLIP.<ver>) that defines the parameters, options, settings, and defaults applicable for the current program.

Port

A port is an assigned number used to uniquely identify a connection endpoint and to route data to a specific service.

RFC (Request for Comment)

Publication series by major technical and standards-setting bodies for the Internet.

rSyslog

Open-source implementation of the Syslog protocol based on the BSD Syslog protocol originally specified in RFC 3164.

SAT (Security Audit Trail)

The logging component of BS2000 for security-relevant events.

SATCP (SAT Control Program)

Subsystem for monitoring events and alarms within SAT.

SATUT

Utility for evaluating and processing SATLOG files.

SERSLOG

Software error logging in BS2000.

SIEM (Security Information and Event Management)

Systems for collecting, monitoring, and analyzing security data.

Socket

An operating system–provided communication endpoint for bidirectional communication between applications.

Subsystem

Within dynamic subsystem management (DSSM), a subsystem is a unit that performs a function and can be loaded, started, and stopped automatically and independently, taking into account dependency relationships with other subsystems. A subsystem can consist of a number of subsystem components.

Syslog (System Logging Protocol)

Standard for message logging in an IP network.

TCP (Transmission Control Protocol)

One of the main protocols of the Internet protocol family. It is a reliable, connection-oriented, packet-switched transport protocol in computer networks.

TCP/IP

Common term for the Internet protocol family.

TPR (Task privileged)

Privileged parts of the BS2000 operating system running in system address space.

TSOS

User ID for the system administrator in the BS2000 system.

TU (Task unprivileged)

Non-privileged parts of the BS2000 operating system, e.g., also user programs.

8 Related publications

You will find the manuals on the internet at http://bs2manuals.ts.fujitsu.com. You can order printed copies of those manuals which are displayed with an order number.

BS2000 OS DX
Accounting Records
User Guide

BS2000 OS DX
DSSM
User Guide

DSSM/SSCM
Subsystem Management in BS2000
User Guide

openNet Server
SOCKETS
User Guide

SECOS
Security Control System - Audit
User Guide