Deutsch

Fujitsu Software BS2000

# CLIP V21.0B10

## Common Logging Interface Provider

## Benutzerhandbuch

Ausgabe Juni 2025

## Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an bs2000services@fujitsu.com senden.

## Zertifizierte Dokumentation nach DIN EN ISO 9001:2015

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001: 2015 erfüllt.

## Copyright und Handelsmarken

# Inhaltsverzeichnis

## CLIP

# 1 Einleitung

CLIP ist ein BS2000-Softwareprodukt zur Integration von BS2000 spezifischen Meldungen, von sicherheitsrelevanten Informationen und Ereignissen, sowie deren zentraler Weiterleitung an ein externes Security-Management System, ein SIEM-System.

Im Betriebssystem BS2000 werden Meldungen und Ereignisse unterschiedlicher Instanzen wie z.B. Security Audit Trail Protokoll (SATLOG-Datei), ACCOUNTING, Konsol-Logging (CONSLOG-Datei), SW Error Logging (SERSLOG-Datei) in unterschiedlichen Dateien protokolliert.

CLIP ist dafür ausgelegt, unterschiedliche Ereignisse im BS2000-System zu sammeln und in das vom Syslog-Protokoll definierte Format (RFC5424) umzuwandeln. Diese Nachrichten werden über Sockets-Verbindungen an einen externen Server gesendet, der das Syslog-Format unterstützt, z.B. ein Linux-rSyslog-Server. Der externe Server kann Ereignisse mehrerer BS2000-Systeme sammeln, filtern und verarbeiten, die im Anschluss von einem SIEM-System aufbereitet werden können.

CLIP unterstützt aktuell BS2000 Ereignisse und Meldungen folgender Instanzen:

- von SAT (Security Audit Trail) protokollierte Ereignisse, die im BS2000 in der SAT-Protokolldatei (SATLOG) aufgezeichnet und im BS2000 mit SATUT ausgewertet werden können.
- ACCOUNTING-Einträge zur Abrechnung

## 1.1 Zielsetzung und Zielgruppen des Handbuchs

Das Handbuch wendet sich an die Systembetreuung und den Service, die das Subsystem CLIP im BS2000 betreiben, sowie an die Administration der Linux-Server, die das Syslog-Protokoll unterstützen.

Die Administration von CLIP setzt umfassende Kenntnisse von BS2000- und Linux-Betriebssystemen voraus.

## 1.2 Konzept des Handbuchs

Das Handbuch beschreibt die grundlegende Struktur, die Funktionen und die Anwendung des Subsystems CLIP.

Das Kapitel "Software-Produkt CLIP" gibt einen Überblick über Struktur, Installation und Konfiguration des Produkts CLIP.

Die Kapitel "CLIP-Architektur" und "Syslog-Protokoll" beschreiben die Architektur und unterstützten Formate zum Einsatz von CLIP.

Am Ende des Handbuchs finden Sie verschiedene Beispiele, die Ihnen das Arbeiten mit diesem Handbuch erleichtern.

## 1.3 Änderungen gegenüber dem Vorgänger-Handbuch

### Änderungen in CLIP V21.0B10

- CLIP unterstützt ACCOUNTING-Einträge
- In der Parameterdatei kann ein Filter für die SATLOG- und ACCOUNTING-Ereignisse konfiguriert werden

### Änderungen in CLIP V21.0B01

- Unterstützung von IPv6 und FQDN
- In der Parameterdatei kann der Parameter LOGSERVER anstelle von IP verwendet werden
- Unterstützung der *EXTENDED-Felder in SAT

## 1.4 Darstellungsmittel

In diesem Handbuch werden die folgenden typographischen Elemente verwendet:

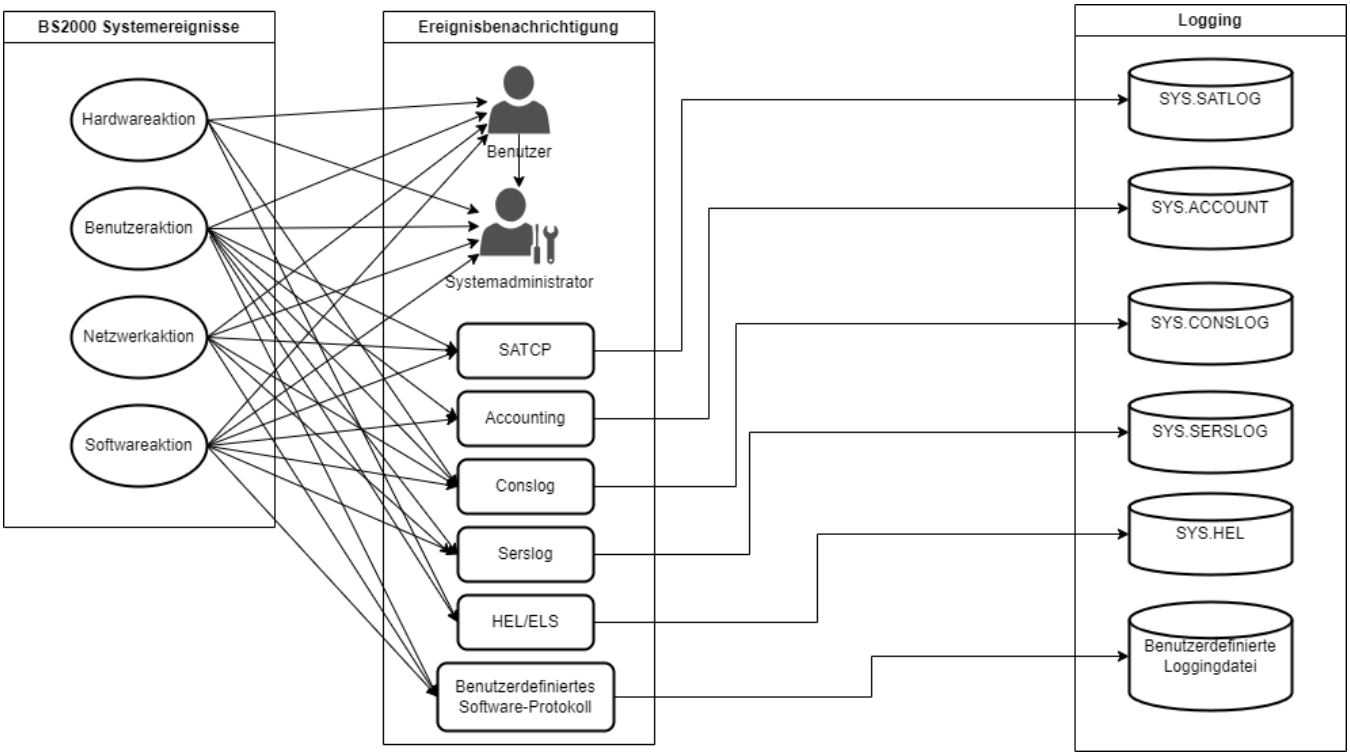
| | |
|---|---|
| **`EINGABE`** | Eingaben in Beispielen erscheinen in fetter Schreibmaschinenschrift. |
| `Ausgabe` | Ausgaben in Beispielen erscheinen in Schreibmaschinenschrift |

# 2 Protokollierung im BS2000-System

Im Betriebssystem BS2000, wie auch in jedem anderen Betriebssystem wird sichergestellt, dass die Systemverwaltung über alle relevanten Ereignisse informiert wird. Relevante Ereignisse können durch Hardware- und/oder Software, wie auch von Benutzeraktionen und automatisierten Prozessen ausgelöst werden.

All diese Ereignisse werden im System von unterschiedlichen Instanzen und in unterschiedlichen Dateien protokolliert. Im BS2000 sind dies z.B. SAT, ACCOUNTING, CONSLOG, etc. Abhängig von der Protokollierungsinstanz werden daher Ereignisse in unterschiedlichen Formaten protokolliert (z.B. in einem binären Format für SAT, oder auch Meldungen in einem abdruckbaren Format in CONSLOG).

Die nachstehende Abbildung stellt die typische Protokollierung des Informationsflusses im Betriebssystem BS2000 dar, die für eine Auswertung in Frage kommen:



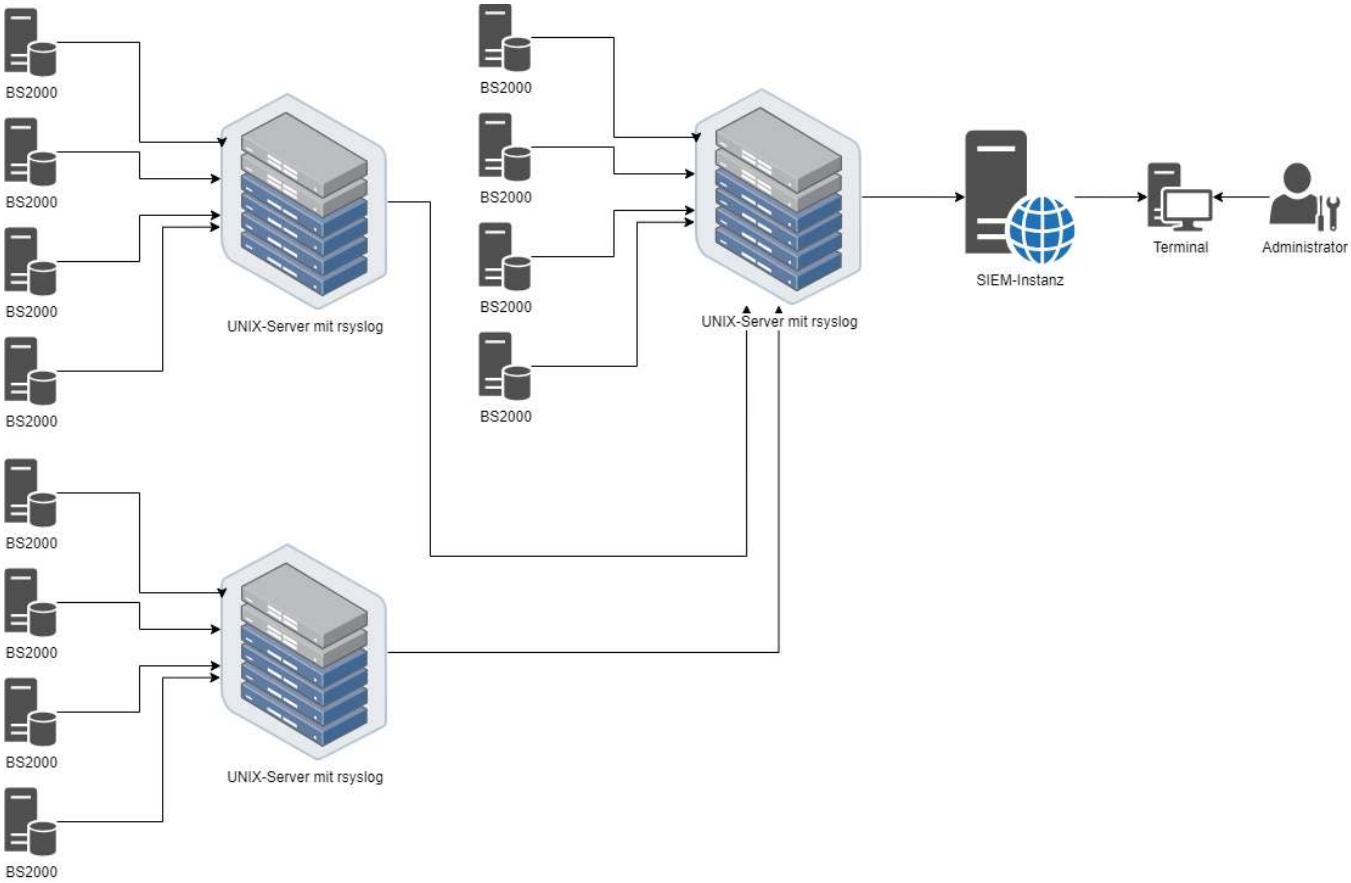

Die Menge der von einem Betriebssystem erzeugten und protokollierten Ereignisse kann beträchtlich sein. Daher werden in internen und externen Protokollierungs- und Auswerte-Tools im BS2000 spezifische Filter- und Auswertefunktionen angeboten und in der BS2000 Dokumentation beschrieben.

Das Subsystem CLIP stellt im BS2000 eine gemeinsame Schnittstelle bereit, die von unterschiedlichen Instanzen produzierte sicherheitsrelevante BS2000 Meldungen und Ereignisse sammelt auf das einheitliche Syslog Protokollformat abbildet und zur Weiterverarbeitung an einem externen Server, wie zum Beispiel einen rSyslog-Server, sendet. Von da können diese dann an eine zentrale SIEM Instanz zur Auswertung weiter geleitet werden.

In der aktuellen Version von CLIP werden für BS2000 diese Ereignisse unterstützt und für eine externe Auswertung bereitgestellt:

- SAT (Security Audit Trail)
- ACCOUNTING (Abrechnungssätze)

Im folgenden dargestellten möglichen Szenario werden als Beispiel rSyslog-Server verwendet. Diese empfangen und speichern die Ereignisse für jeweils mehrere BS2000-Systeme. Die rSyslog-Server selber können auch kaskadieren, also die Ereignisse auch an einen zentralen rSyslog-Server weiterleiten, der wiederum alle Ereignisse sammelt, um sie im Anschluss z.B. an eine SIEM-Instanz zur Auswertung zu senden. Das in diesem Beispiel dargestellte Szenario verdeutlicht die Skalierbarkeit der Infrastruktur.



# 3 Syslog-Protokoll

Das ursprüngliche Syslog-Protokoll wurde in RFC 3164 definiert. Da es jedoch keine offizielle Standardisierung erfuhr, wurde mit RFC 5424 ein neuer Standard veröffentlicht, der die Spezifikation präzisiert und erweitert. CLIP überträgt Nachrichten ausschließlich im Format von RFC 5424. Die Konfiguration erfolgt dabei mit den Parametern facility: 1 (Nachrichten auf Benutzerebene) und severity: 6 (informativ).

Feldbezeichnungen und Werte werden auf durch ein Leerzeichen getrennte "Feldbezeichnung"="Wert"-Paare abgebildet.

Die verschiedenen Wertetypen werden wie folgt formatiert und im ASCII-Code übertragen:

- c-Strings bleiben unverändert
- Zahlen werden als Zeichenfolgen von Ziffern dargestellt (0..9)
- x-Strings werden als Zeichenfolgen von Ziffern und Buchstaben dargestellt (0..9A..F)
- Schlüsselwörter werden in ihre Bedeutung übersetzt

CLIP verarbeitet derzeit sicherheitsrelevante BS2000 Ereignisse und Meldungen folgender Instanzen und überträgt sie im RFC-5424-konformen Syslog-Format an einen externen Server, wie zum Beispiel einen rSyslog-Server:

- **SAT (Security Audit Trail)**
  Feldbezeichnungen und Werte sind im SECOS-Handbuch dokumentiert.

  > **Hinweis**
  > HEADER- und TRAILER-Satz einer SAT-Datei werden direkt in die Datei geschrieben. Die zugehörigen SAT-Events ZBG und ZND werden deshalb nicht an CLIP übertragen und können dort nicht protokolliert werden.

- **ACCOUNTING (Abrechnungseinträge)**
  Details folgen im nächsten Abschnitt.

rSyslog ist ein weit verbreitetes Open-Source-Tool zur Weiterleitung von Lognachrichten auf Basis des Syslog-Protokolls.

Das von CLIP genutzte Meldungsformat wird nachfolgend beschrieben. Die Beschreibung der Abschnitte der Kopfzeile ist in RFC5424 spezifiziert.

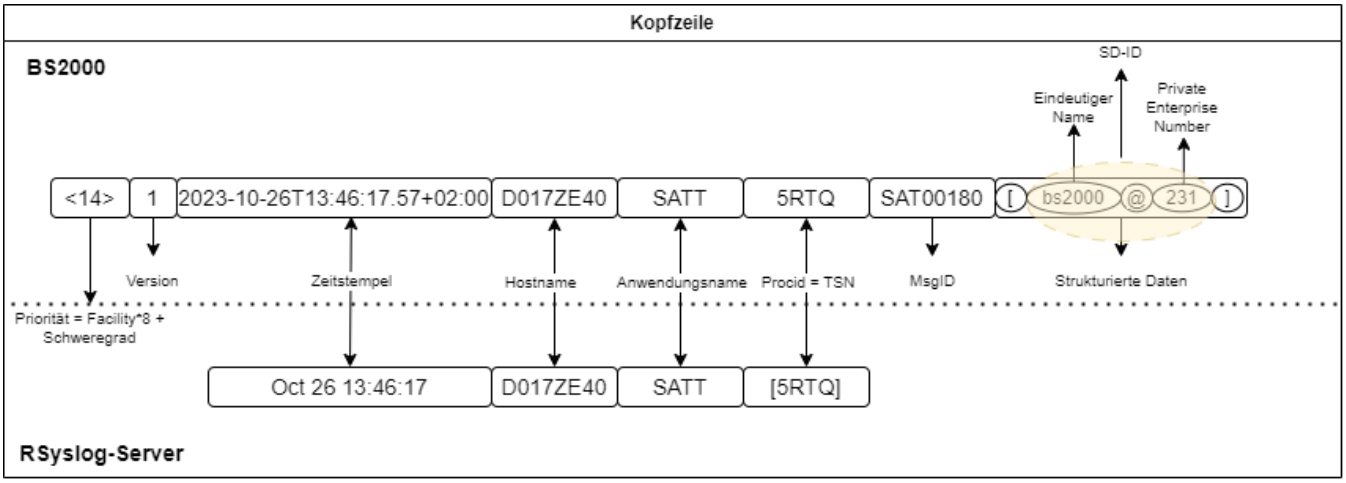
Beispiel für eine von CLIP über die Netzwerkschnittstelle übermittelte Syslog-Nachricht:

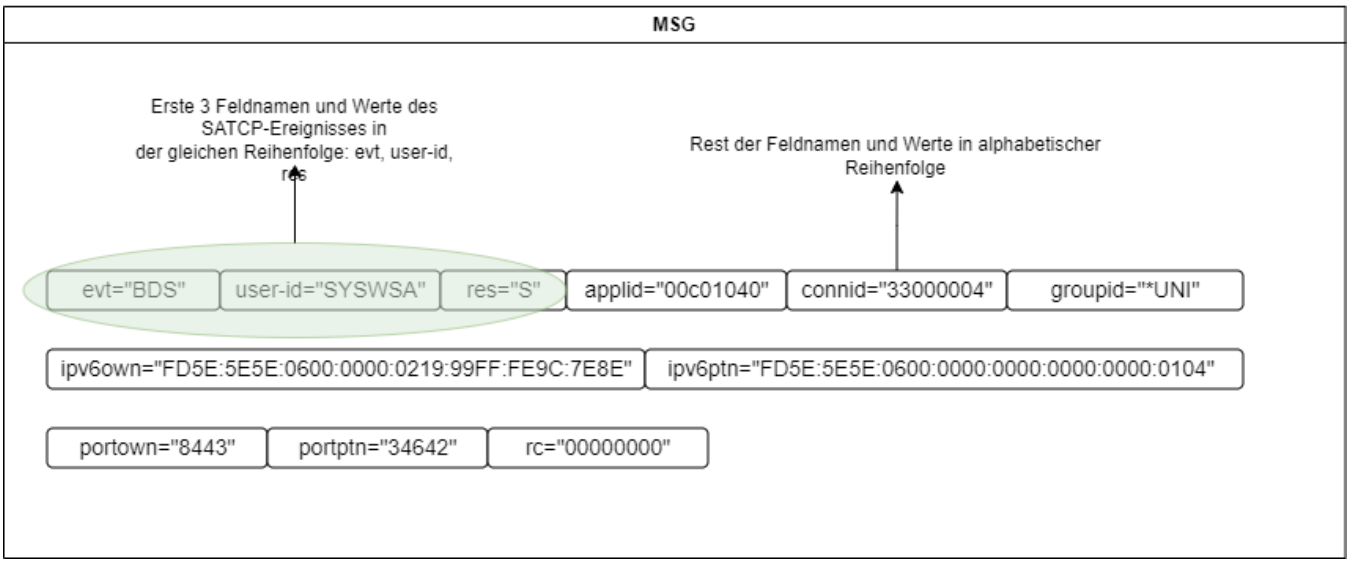
```
<14>1 2023-10-26T13:46:17.57+02:00 D017ZE40 SATT 5RTQ SAT00180 [bs2000@231] evt="
BDS" user-id="SYSWSA" res="S" applid="00c01040" connid="33000004" groupid="*UNI"
ipv6own="FD5E:5E5E:0600:0000:0219:99FF:FE9C:7E8E" ipv6ptn="FD5E:5E5E:0600:0000:0000:
0000:0000:0104" portown="8443" portptn="34642" rc="00000000"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

Beispiel für die Darstellung dieser Nachricht von einem 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"
```

Das Format der Nachricht wird in den folgenden Abbildungen dargestellt:


Kopfzeile
BS2000
SD-ID
Eindeutiger Name
Private Enterprise Number
<14>
1
2023-10-26T13:46:17.57+02:00
D017ZE40
SATT
5RTQ
SAT00180
[
bs2000
@
231
]
Version
Zeitstempel
Hostname
Anwendungsname
Procid = TSN
MsgID
Strukturierte Daten
Priorität = Facility*8 + Schweregrad
Oct 26 13:46:17
D017ZE40
SATT
[5RTQ]
RSyslog-Server


MSG
Erste 3 Feldnamen und Werte des SATCP-Ereignisses in der gleichen Reihenfolge: evt, user-id, res
Rest der Feldnamen und Werte in alphabetischer Reihenfolge
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 der nachfolgenden Tabelle werden die einzelnen Felder der ACCOUNTING-Abrechnungssätze genauer definiert. Weitere Informationen finden Sie im Handbuch "Abrechnungssätze" sowie in den entsprechenden spezifischen Manualen (siehe dazu auch die Übersicht der Abrechnungssätze in "Einführung in die Systembetreuung").

Für Feldnamen die mit einem <x> gelistet sind gilt:

Dem Feldnamen wird bei manchen Abrechnungssätzen ein Prefix bestehend aus 2 Buchstaben und ein Suffix bestehend aus einer aufsteigenden Zahl aus 2 Ziffern angehangen.
Beispiel: Das Feld 1 wird als "userid<x>" gelistet. Die beiden Abrechnungssätze DSPC und DSPP verwenden dieses Feld variabel, weswegen bei diesen Abrechnungssätzen ein Prefix und Suffix angehangen wird. Die vollständigen Feldnamen für diese beiden Abrechnungssätze lauten dann wie folgt:

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

Alle anderen Abrechnungssätze verwenden nur den statischen Namen, daher heißt das Feld z.B. bei dem Abrechnungssatz "JOBS": userid

| Feld-ID | Feldname | Feld-Beschreibung | Mögliche Abrechnungssätze mit diesem Feld |
|---|---|---|---|
| 1 | userid<x> | Benutzerkennung | JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS<COx>, DSPC<SPx>, DSPP<PSx>, DRFA, FTR0, SOPA |
| 2 | accnr<x> | Abrechnungsnummer | 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 | Gruppenname | JOBS, TASK, PRGS, PRGT, PACC, PDMP, SPLO, TDEV, TATR, UDAT, UACC, HSMS, DRFA, FTR0, SOPA |
| 5 | ident | Pubset-Kennzeichen "PUB" | DSPC, DALC |
| 6 | catid | Katalogkennung | DSPC, DALC, AOPN, ACLS |
| 7 | ownerid | Eigentümer-Kennung | DSPC, DALC |
| 8 | vsn | VSN der Platte | DSPP, DRVR |
| 9 | mnemonic | Mnemotechnischer Name der Platte | DSPP |
| 10 | install | Anlagenbezeichnung | AOPN, ACLS |
| 11 | osname | Betriebssystemname | AOPN, ACLS |
| 12 | osver | Betriebssystemversion | AOPN, ACLS |
| 13 | session | Session-Nummer | AOPN, ACLS |

| | | | |
|---|---|---|---|
| 14 | maxcpu | 'E' bei mehr als 8 CPU-IDs | AOPN, ACLS |
| 15 | install2 | Anlagen-Identifikation | AOPN, ACLS |
| 16 | intface | Hardware-Software-Interface | AOPN, ACLS |
| 17 | cpuid1 | CPU-IDs 1-8 | AOPN, ACLS |
| 18 | cpuid2 | CPU-IDs 9-16 | AOPN, ACLS |
| 19 | extvers | Erweiterte Versionsbezeichnung | AOPN, ACLS |
| 23 | subname | Name des Subsystems | ESMC, ESMD |
| 24 | subvers | Subsystem-Version | ESMC, ESMD |
| 25 | calldat | Datum des Aufrufs | ESMC, ESMD |
| 26 | calltim | Uhrzeit des Aufrufs | ESMC, ESMD |
| 27 | jobacdat | Datum der Job-Annahme | JOBS |
| 28 | jobactim | Uhrzeit der Job-Annahme | JOBS |
| 29 | jobstdat | Datum des Job-Starts | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 30 | jobsttim | Uhrzeit des Job-Starts | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 31 | jobname | Jobname | JOBS, SPLI |
| 32 | jobaccen | Jahrhundert Job-Annahme | JOBS |
| 33 | jobstcen | Jahrhundert Job-Start | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 34 | jobacsea | Kennzeichen Jahreszeit für Job-Annahme | JOBS |
| 35 | jobstsea | Kennzeichen Jahreszeit für Job-Start | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 36 | tsktmdat | Datum der Task-Beendigung | TASK |
| 37 | tsktmtim | Uhrzeit der Task-Beendigung | TASK |
| 38 | tskcpu | Task-CPU-Zeit | TASK, PRGS, PRGT, PACC, UACC, HSMS, RCPU, SOPA |
| 39 | inoutnr<x> | Anzahl der Ein/Ausgaben | TASK, PRGS, PRGT, PACC, UACC, HSMS, TDEV<DUx, DVx, VUx>, SOPA |
| 40 | dattrans<x> | Übertragene Datenmenge | TASK, PRGS, PRGT, PACC, UACC, TDEV<DUx, DVx, VUx> |
| 41 | mainmem | Hauptspeicherbelegungs-Integral | TASK, PRGS, PRGT, PACC, UACC |
| 42 | resmem | Residenter Memory Pool-Integral | TASK, PRGS, PRGT, PACC, UACC |
| 43 | pagingnr | Anzahl der Seitenwechsel | TASK, PRGS, PRGT, PACC, UACC |
| 44 | tskprio | Task-Scheduling-Priorität | JOBS, TASK, PRGS, PRGT, PACC, UACC |

| | | | |
|---|---|---|---|
| 45 | tskatt | Task-Scheduling-Attribut | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 46 | secmoutm | SECURE- und MOUNT-Wartezeit | TASK, PRGS, PRGT, PACC, UACC |
| 47 | tsktype | Task-Kategorie | JOBS, TASK, PRGS, PRGT, PACC, UACC |
| 48 | jobtmcen | Jahrhundert Job-Beendigung | TASK |
| 49 | vecpages | Vektor-Seiten-Integral | TASK, PRGS, PRGT, PACC, UACC |
| 50 | resspace | Residenter DATA SPACE-Integral | TASK, PRGS, PRGT, PACC, UACC |
| 51 | jobtmsea | Kennzeichen Jahreszeit für Job-Ende | TASK |
| 52 | stdcpu | normierte CPU-Zeit | TASK, PRGS, PRGT, PACC, UACC |
| 53 | 390mode | /390-Mode-Zeit | TASK, PRGS, PRGT, PACC, UACC |
| 54 | prgstdat | Datum des Programm-Starts | PRGS |
| 55 | prgsttim | Uhrzeit des Programm-Starts | PRGS |
| 56 | prgstcen | Jahrhundert des Programm-Starts | PRGS |
| 57 | prgstsea | Kennzeichen Jahreszeit für Programm-Start | PRGS |
| 58 | prgtmdat | Datum der Programm-Beendigung | PRGT |
| 59 | prgtmtim | Uhrzeit der Programm-Beendigung | PRGT |
| 60 | prgtmcen | Jahrhundert der Programm-Beendigung | PRGT |
| 61 | prgtmsea | Kennzeichen Jahreszeit für Programm-Ende | PRGT |
| 62 | recdat | Datum der Programm-Erfassung | PACC, UACC, RCPU |
| 63 | rectim | Uhrzeit der Programm-Erfassung | PACC, UACC, RCPU |
| 64 | reccen | Jahrhundert der Programm-Erfassung | PACC |
| 65 | recsea | Kennzeichen Jahreszeit für Schreiben des Satzes | PACC |
| 66 | dumpsdat | Datum des Dump-Starts | PDMP |
| 67 | dumpstim | Uhrzeit des Dump-Starts | PDMP |
| 68 | dumpedat | Datum der Dump-Beendigung | PDMP |

| | | | |
|---|---|---|---|
| 69 | dumpetim | Uhrzeit der Dump-Beendigung | PDMP |
| 70 | dumppag | Anzahl der ausgegebenen Arbeitsspeicherseiten | PDMP |
| 71 | dumptsk | TSN der Dump-Task | PDMP |
| 72 | crashtsk | TSN der betroffenen Task | PDMP |
| 73 | splosdat | Datum des SPOOLOUT-Starts | SPLO |
| 74 | splostim | Uhrzeit des SPOOLOUT-Starts | SPLO |
| 75 | sploedat | Datum der SPOOLOUT-Beendigung | SPLO |
| 76 | sploetim | Uhrzeit der SPOOLOUT-Beendigung | SPLO |
| 77 | splonam | SPOOLOUT-Auftragsname | SPLO |
| 78 | copycnt | Anzahl der noch auszugebenden Kopien | SPLO |
| 79 | splocls | SPOOLOUT-Klasse | SPLO |
| 80 | sploprio | SPOOLOUT-Scheduling-Priorität | SPLO |
| 81 | splotype | Art der SPOOLOUT-Datei | SPLO |
| 82 | sploscen | Jahrhundert für SPOOLOUT-Start | SPLO |
| 83 | splossea | Kennzeichen Jahreszeit für SPOOLOUT-Start | SPLO |
| 84 | sploesea | Kennzeichen Jahreszeit für SPOOLOUT-Ende | SPLO |
| 85 | sploecen | Jahrhundert für SPOOLOUT-Ende | SPLO |
| 86 | prnttsn | TSN des Partner-Druckauftrages | SPLO |
| 87 | reldat | Datum der Freigabe | TDEV |
| 88 | reltim | Uhrzeit der Freigabe | TDEV |
| 89 | relcen | Jahrhundert der Freigabe | TDEV |
| 90 | relsea | Kennzeichen Jahreszeit für Freigabe | TDEV |
| 91 | tskmddat | Datum der Task-Änderung | TATR |
| 92 | tskmdtim | Uhrzeit der Task-Änderung | TATR |

| | | | |
|---|---|---|---|
| 93 | tskmdpri | Neue Task-Scheduling-Priorität | TATR |
| 94 | tskmdatt | Neues Task-Scheduling-Attribut | TATR |
| 95 | tskmdcen | Jahrhundert der Task-Änderung | TATR |
| 96 | tskmdsea | Kennzeichen Jahreszeit für Task-Änderung | TATR |
| 97 | stktime | Datum und Uhrzeit der Bestandsaufnahme | DSPC, DSPP |
| 98 | compstat | Anzeige für Vollständigkeit | DSPC |
| 99 | curcen | Jahrhundert (aktuell) | UACC, DSPC, DALC, DSPP, RCPU |
| 100 | cursea | Kennzeichen Jahreszeit für aktuelle Zeit | UACC, DSPC, DSPP, ESMC, ESMD, RCPU |
| 101 | recavdat | Datum der Satzbereitstellung | DALC |
| 102 | udatdat | Datum des Benutzerdaten-Aufrufs | UDAT |
| 103 | udatim | Uhrzeit des Benutzerdaten-Aufrufs | UDAT |
| 104 | udatcen | Jahrhundert des Benutzerdaten-Aufrufs | UDAT |
| 105 | udatsea | Kennzeichen Jahreszeit für Benutzerdaten-Aufruf | UDAT |
| 106 | sysidat | Datum der Systemeinleitung | AOPN |
| 107 | sysitim | Uhrzeit der Systemeinleitung | AOPN |
| 108 | filodat | Datum der Dateieröffnung | AOPN |
| 109 | filotim | Uhrzeit der Dateieröffnung | AOPN |
| 110 | filorea | Grund für die Dateieröffnung | AOPN |
| 111 | sysicen | Jahrhundert der Systemeinleitung | AOPN |
| 112 | filocen | Jahrhundert der Dateieröffnung | AOPN |
| 113 | sysisea | Kennzeichen Jahreszeit für Systemeinleitung | AOPN |
| 114 | filosea | Kennzeichen Jahreszeit für Dateieröffnung | AOPN |
| 115 | timezon | Zeitzone | AOPN |
| 116 | timediff | Zeitdifferenz | AOPN |

| | | | |
|---|---|---|---|
| 117 | filcdat | Datum der Dateischließung | ACLS |
| 118 | filctim | Uhrzeit der Dateischließung | ACLS |
| 119 | filcrea | Grund für die Dateischließung | ACLS |
| 120 | filccen | Jahrhundert der Dateischließung | ACLS |
| 121 | filcsea | Kennzeichen Jahreszeit für Dateischließung | ACLS |
| 122 | intcpu | Unterbrechungsanalyse-CPU-Zeit | RCPU |
| 123 | idlecpu | CPU-IDLE-Zeit | RCPU |
| 124 | spoolid | "SPOOLOUT" | RSRV |
| 125 | spooldev | Art des SPOOLOUT-Gerätes | RSRV |
| 126 | spoolmne | Mnemotechnischer Name des SPOOLOUT-Gerätes | RSRV |
| 127 | spooltsn | TSN der SPOOLOUT-Treibertask | RSRV |
| 128 | substati | Zustandsanzeige Subsystem-Initialisierung | ESMC |
| 129 | substatt | Zustandsanzeige Subsystem-Beendigung | ESMD |
| 256 | extid1 | Erweiterungskennung 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 | Erweiterungskennung 2 | JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, AOPN, ACLS, RSRV, HSMS, BCA4, SPLI, FTR0 |
| 258 | extid3 | Erweiterungskennung 3 | JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, AOPN, HSMS, BCA4, FTR0 |
| 259 | extid4 | Erweiterungskennung 4 | JOBS, TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, FTR0 |
| 260 | extid5 | Erweiterungskennung 5 | TASK, PRGS, PRGT, PACC, SPLO, UACC |
| 261 | extid6 | Erweiterungskennung 6 | TASK, PRGS, PRGT, PACC, SPLO, UACC |
| 262 | extid7 | Erweiterungskennung 7 | TASK, PRGS, PRGT, PACC, SPLO |
| 263 | extid8 | Erweiterungskennung 8 | PRGT |
| 264 | extid9 | Erweiterungskennung 9 | - |
| 266 | extcase | Fallkennzeichen | JOBS, SPLO, RSRV |
| 272 | joborig | Herkunft des Auftrags | JOBS |
| 273 | jobcrea | Erzeuger des Auftrags | JOBS |

| | | | |
|---|---|---|---|
| 274 | jservnam | Name des Herkunftsservers für den Auftrag | JOBS |
| 275 | jcreatsn | TSN des erzeugenden Auftrags | JOBS, SPLO |
| 276 | diatype | Art des Dialog-Partners | JOBS |
| 277 | servnam | Name des Servers | JOBS |
| 278 | termapp | Name Datensichtstation oder Anwendung | JOBS |
| 279 | termtyp | Stationstyp | JOBS |
| 280 | repcnt | Wiederholungszähler | JOBS |
| 281 | subsid | Kennzeichnung des "Subsystems" | JOBS |
| 282 | jobclass | Jobklasse | JOBS |
| 283 | jobprio | Job-Scheduling-Priorität | JOBS |
| 284 | jobsinf | Jobstart-Angaben | JOBS |
| 285 | cputimel | Angefordertes CPU-Zeit-Limit | JOBS |
| 286 | printlim | Angefordertes PRINT-Limit | JOBS |
| 287 | punchlim | Angefordertes PUNCH-Limit | JOBS |
| 288 | jobpar | Job-Parameter | JOBS |
| 289 | termrea<x> | Beendigungs-Anzeige | TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx> |
| 290 | termunit | Beendigungs-Einheit | TASK, PRGT |
| 291 | termorig<x> | Beendigungs-Herkunft | TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx> |
| 292 | termcode<x> | Beendigungscode | TASK, PRGT, SPLO, DRFA<STx>, SRBS<STx>, SPLI<ITx> |
| 293 | cl56mem | Summe Klasse 5 und 6 Speicherbelegung | TASK, PRGS, PRGT, PACC, UACC |
| 294 | commem | Common Memory Pool Integral | TASK, PRGS, PRGT, PACC, UACC |
| 295 | eammem | EAM-Speicher-Belegung | TASK, PRGS, PRGT, PACC, UACC |
| 296 | datspace | DATA-SPACE-Integral | TASK, PRGS, PRGT, PACC, UACC |
| 297 | iopubvol | Anzahl E/A für Public Volume Sets | TASK, PRGS, PRGT, PACC, UACC, HSMS |
| 298 | ioshprv | Anzahl E/A für shareable Privatplatten | TASK, PRGS, PRGT, PACC, UACC, HSMS |
| 299 | ioexprv | Anzahl E/A für exklusive Privatplatten | TASK, PRGS, PRGT, PACC, UACC, HSMS |

| | | | |
|---|---|---|---|
| 300 | iomtape | Anzahl E/A für Magnetbänder | TASK, PRGS, PRGT, PACC, UACC, HSMS |
| 301 | iorecdev | Anzahl E/A für Nicht-Volume-Geräte | TASK, PRGS, PRGT, PACC, UACC, HSMS |
| 302 | dtpubvol | Übertragene Daten für Public Volume Sets | TASK, PRGS, PRGT, PACC, UACC |
| 303 | dtshprv | Übertragene Daten für shareable Privatplatten | TASK, PRGS, PRGT, PACC, UACC |
| 304 | dtexprv | Übertragene Daten für exklusive Privatplatten | TASK, PRGS, PRGT, PACC, UACC |
| 305 | dtmtape | Übertragene Daten für Magnetbänder | TASK, PRGS, PRGT, PACC, UACC |
| 306 | dtrecdev | Übertragene Daten für Nicht-Volume-Geräte | TASK, PRGS, PRGT, PACC, UACC |
| 307 | iotermlo | Anzahl der Terminal-E/A (low) | TASK, PRGS, PRGT, PACC, UACC |
| 308 | dttermlo | Anzahl übertragene Bytes am Terminal (low) | TASK, PRGS, PRGT, PACC, UACC |
| 309 | iotermhi | Anzahl der Terminal-E/A (high) | TASK, PRGS, PRGT, PACC, UACC |
| 310 | dttermhi | Anzahl übertragene Bytes am Terminal (high) | TASK, PRGS, PRGT, PACC, UACC |
| 311 | locfiacc | Anzahl Katalogzugriffe zu lokalen Dateien | TASK, PRGS, PRGT, PACC, UACC |
| 312 | locjvacc | Anzahl Katalogzugriffe zu lokalen Jobvariablen | TASK, PRGS, PRGT, PACC, UACC |
| 313 | remfiacc | Anzahl Katalogzugriffe zu remote Dateien | TASK, PRGS, PRGT, PACC, UACC |
| 314 | remjvacc | Anzahl Katalogzugriffe zu remote Jobvariablen | TASK, PRGS, PRGT, PACC, UACC |
| 315 | dynserrq | Maximale dynamische SERVICE-RATE-Anforderung | TASK, PRGS, PRGT, PACC, UACC |
| 316 | spservlo | Abgegebene SERVICE-UNITS (low) | TASK, PRGS, PRGT, PACC, UACC |
| 317 | spcpulo | Abgegebene CPU-SU (low) | TASK, PRGS, PRGT, PACC, UACC |
| 318 | spiolo | Abgegebene IO-SU (low) | TASK, PRGS, PRGT, PACC, UACC |
| 319 | spmemlo | Abgegebene MEMORY-SU (low) | TASK, PRGS, PRGT, PACC, UACC |
| 320 | spservhi | Abgegebene SERVICE-UNITS (high) | TASK, PRGS, PRGT, PACC, UACC |
| 321 | spcpuhi | Abgegebene CPU-SU (high) | TASK, PRGS, PRGT, PACC, UACC |
| 322 | spiohi | Abgegebene IO-SU (high) | TASK, PRGS, PRGT, PACC, UACC |

| | | | |
|---|---|---|---|
| 323 | spmemhi | Abgegebene MEMORY-SU (high) | TASK, PRGS, PRGT, PACC, UACC |
| 324 | stdcpusu | Normierte CPU-SU | TASK, PRGS, PRGT, PACC, UACC |
| 325 | stdservu | Normierte SERVICE UNITS | TASK, PRGS, PRGT, PACC, UACC |
| 326 | accid | Account-ID | TASK, PRGS, PRGT, PACC, SPLO, TDEV, UACC, HSMS |
| 327 | progorig | Anzeige für Programm-Herkunft | PRGS |
| 328 | resrea | RESTART-Anzeige | PRGS |
| 329 | proginf | Zusatzinformationen zur Programm-Herkunft | PRGS |
| 330 | prgversh | Programm-Version (10 Zeichen) | PRGS |
| 331 | prgname | Programm- oder Modulname | PRGS |
| 332 | prgvercp | Programm-Version (komplett) | PRGS |
| 333 | filenam | Dateiname | PRGT |
| 334 | elemnam | Elementname | PRGT, SPLO |
| 335 | elemver | Elementversion | PRGT, SPLO |
| 336 | elemtyp | Elementtyp | PRGT, SPLO |
| 337 | prevdat | Datum des vorhergehenden PACC-Satzes | PACC |
| 338 | prevtim | Zeit des vorhergehenden PACC-Satzes | PACC |
| 339 | prevcen | Jahrhundert des vorhergehenden PACC-Satzes | PACC |
| 340 | prevsea | Jahreszeit des vorhergehenden PACC-Satzes | PACC |
| 341 | splocrea | Datum und Uhrzeit des SPOOLOUT-Auftrags | SPLO |
| 342 | origuser | Ursprüngliche Benutzerkennung (bei Replay-Jobs) | SPLO |
| 343 | tapedev | Mnemotechnischer Name des Bandgerätes | SPLO |
| 344 | printdev | Mnemotechnischer Name des Druckers | SPLO |
| 345 | linecnt | Anzahl der gedruckten Zeilen | SPLO, RSRV, SRBS |

| | | | |
|---|---|---|---|
| 346 | pagecnt | Anzahl der gedruckten Seiten | SPLO |
| 347 | devname | Gerätename | SPLO |
| 348 | formname | FORM-Name | SPLO |
| 349 | compid | Komponenten-Kennzeichen | SPLO |
| 350 | devmnem<x> | Mnemotechnischer Gerätename | 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 | Verbrauchte Zeit (.01 Sek.) | SPLO |
| 355 | #pagedef | Anzahl angeforderter PAGEDEF | SPLO |
| 356 | #formdef | Anzahl angeforderter FORMDEF | SPLO |
| 357 | #fontsrq | Anzahl angeforderter FONTS | SPLO |
| 358 | #fontsld | Anzahl geladener FONTS | SPLO |
| 359 | #overlrq | Anzahl angeforderter Dias | SPLO |
| 360 | #overlld | Anzahl geladener Dias | SPLO |
| 361 | #pagused | Größe benutzter Seiten | SPLO |
| 362 | flginp | Eingabefachmaske | SPLO |
| 363 | flgout | Ausgabefachmaske | SPLO |
| 364 | flgdup | Marke für doppelseitigen Druck | SPLO |
| 365 | splofil | Dateiname der SPOOLOUT-Datei | SPLO |
| 366 | reccnt | Anzahl der Sätze | SPLO |
| 367 | devtype<x> | Gerätetyp | TDEV<DUx, DVx, VUx>, VACD, SPLI |
| 368 | occtime<x> | Datum und Uhrzeit des Belegungsbeginns | TDEV<DUx, DVx, VUx> |
| 369 | alloctyp<x> | Belegungsart | TDEV<DUx, DVx, VUx> |
| 370 | alloccen<x> | Jahrhundert (Beginn Belegung) | TDEV<DUx, DVx, VUx> |
| 371 | allocsea<x> | Kennzeichen Jahreszeit für Belegungsbeginn | TDEV<DUx, DVx, VUx> |
| 372 | volser#<x> | Datenträgerkennzeichen | TDEV<VUx> |

| | | | |
|---|---|---|---|
| 373 | rdwrind<x> | Lese-/Schreib-Indikator (U/R /W) | TDEV<VUx> |
| 374 | pams0occ<x> | Anzahl belegter PAM-Blöcke Level S0 | DSPC<SPx> |
| 375 | pams1occ<x> | Anzahl belegter PAM-Blöcke Level S1 | DSPC<SPx> |
| 376 | pams2occ<x> | Anzahl belegter PAM-Blöcke Level S2 | DSPC<SPx> |
| 377 | occpag#<x> | Anzahl der belegten Seiten | DSPP<PSx> |
| 378 | catfil#<x> | Anzahl der katalogisierten Dateien | DSPP<PSx> |
| 379 | mduserid<x> | Betroffene Benutzerkennung | DALC<ALx> |
| 380 | pamoccto<x> | Anzahl der belegten PAM-Blöcke | DALC<ALx> |
| 381 | spacemdv<x> | Wert der Speicherplatz-Änderung | DALC<ALx> |
| 382 | reqtsn<x> | TSN der verursachenden Task | DALC<ALx> |
| 383 | moddate<x> | Datum der Änderung | DALC<ALx> |
| 384 | modtime<x> | Uhrzeit der Änderung | DALC<ALx> |
| 385 | spacetyp<x> | Speicherplatz-Typ | DALC<ALx> |
| 386 | sysid<x> | System-Kennzeichen | DALC<ALx> |
| 387 | modsea<x> | Kennzeichen Jahreszeit für Änderung | DALC<ALx> |
| 388 | userdat | Benutzerdaten | UDAT |
| 389 | pfilenam | Dateiname der Vorgängerdatei | AOPN |
| 390 | mainmems | Hauptspeichergröße | AOPN |
| 391 | pagemems | Größe des seitenwechselbaren Speichers | AOPN |
| 392 | sysspadd | Beginn des Systemadressraums | AOPN |
| 393 | sysspsz | Größe des Systemadressraums | AOPN |
| 394 | cpuidx | CPU-IDs 17-X | AOPN, ACLS |
| 395 | sfilenam | Name der Nachfolgerdatei | ACLS |
| 396 | splocnt | Anzahl der SPOOLOUT-Vorgänge | RSRV, SRBS |

| | | | |
|---|---|---|---|
| 397 | bytecnt | Anzahl der gedruckten Bytes | RSRV, SRBS |
| 398 | servsdat | Datum des Auftragnehmer-Starts | RSRV |
| 399 | servstim | Uhrzeit des Auftragnehmer-Starts | RSRV |
| 400 | servedat | Datum der Auftragnehmer-Task-Beendigung | RSRV |
| 401 | servetim | Uhrzeit der Auftragnehmer-Task-Beendigung | RSRV |
| 402 | ordrtime | Zeitstempel des Auftrags | HSMS |
| 403 | taskid | Kennung des Aufgabentyps | HSMS |
| 404 | tsnrun | TSN der laufenden Aufgabe | HSMS |
| 405 | recindex | Datensatzindex | HSMS, SOPA |
| 406 | accnrlen<x> | Länge der Abrechnungsnummer von Sammelaufträgen | HSMS<COx> |
| 407 | accnr<x> | Abrechnungsnummer von Sammelaufträgen | HSMS<COx> |
| 408 | ownproc | Eigener Prozessorname | BCA4 |
| 409 | ownappl | Eigener Anwendungsname | BCA4 |
| 410 | ownproc# | Eigene Prozessornummer | BCA4 |
| 411 | ownreg | Eigene Regionsnummer | BCA4 |
| 412 | ownlan | Eigene LAN-Adresse | BCA4 |
| 512 | vmindex | VM Index | VACD, VACM |
| 513 | vmname | VM Name | VACD, VACM |
| 514 | vmreldat | Veröffentlichungsdatum der Geräte | VACD |
| 515 | vmreltim | Veröffentlichungszeit der Geräte | VACD |
| 516 | vmrelcen | Jahrhundert der Veröffentlichung der Geräte | VACD |
| 517 | vmrelsea | Saisonkennung für die Veröffentlichung der Geräte | VACD |
| 518 | vmedat | Datum des VM-Stopps | VACM |
| 519 | vmetim | Uhrzeit des VM-Stopps | VACM |
| 520 | vmsdat | Datum des VM-Starts | VACM |
| 521 | vmstim | Uhrzeit des VM-Starts | VACM |

| | | | |
|---|---|---|---|
| 522 | usecpus | Verbrauchte CPU-Zeit in Sekunden | VACM |
| 523 | usecpums | Verbrauchte CPU-Zeit in Mikrosekunden | VACM |
| 524 | memsizmb | Speichergröße in MB | VACM |
| 525 | strsizmb | Erweiterte Speichergröße in MB | VACM |
| 526 | vmecen | Jahrhundert des VM-Stopps | VACM |
| 527 | vmscen | Jahrhundert des VM-Starts | VACM |
| 528 | vmesea | Saisonkennung des VM-Stopps | VACM |
| 529 | vmssea | Saisonkennung des VM-Starts | VACM |
| 530 | rescpus | Reservierte CPU-Zeit in Sekunden | VACM |
| 531 | rescpums | Reservierte CPU-Zeit in Mikrosekunden | VACM |
| 532 | memsizho | Speichergröße in High-Order-Bytes | VACM |
| 533 | strsizho | Erweiterte Speichergröße in High-Order-Bytes | VACM |
| 534 | utmapp | Anwendungsname der UTM-Anwendung | UTMA, UTMK |
| 535 | utmuser | Name des UTM-Benutzers | UTMA, UTMK |
| 536 | signtim | Anmeldezeit | UTMA |
| 537 | utmtime | Datum und Uhrzeit der Protokollerstellung | UTMA |
| 538 | utmaccnt | Zähler der Abrechnungseinheiten | UTMA |
| 539 | utmtacnt | Anzahl der TACs mit TACUNIT > 0 | UTMA |
| 540 | utmtrans | Transaktionscode der Programmeinheit | UTMK |
| 541 | utmcpu | CPU-Zeit in openUTM in Millisekunden | UTMK |
| 542 | dtsyscpu | CPU-Zeit im Datenbanksystem in Millisekunden | UTMK |
| 543 | utmio | Anzahl der IOs in openUTM | UTMK |

| | | | |
|---|---|---|---|
| 544 | dtsysio | Anzahl der IOs im Datenbanksystem | UTMK |
| 545 | msinlen | Länge der Eingabemeldung | UTMK |
| 546 | msoutlen | Länge der Ausgabemeldung | UTMK |
| 547 | asynout | Anzahl asynchroner Ausgaben | UTMK |
| 548 | accltac | Abrechnungseinheiten für LTACs | UTMK |
| 549 | ltermnam | Name des LTERM-Partners | UTMK |
| 550 | progrtim | Echtzeit der Programmeinheitsausführung in Millisekunden | UTMK |
| 551 | mnemfir | Mnemonik des ersten Geräts | DRVR |
| 552 | mnemsec | Mnemonik des zweiten Geräts | DRVR |
| 553 | evtype | Ereignistyp | DRVR |
| 554 | spacetim | Zeitstempel von SPACEOPT | SOPA |
| 555 | rfasdat | Datum der RFA-Verbindungsherstellung | DRFA |
| 556 | rfastim | Uhrzeit der RFA-Verbindungsherstellung | DRFA |
| 557 | rfaedat | Datum des RFA-Sitzungsendes | DRFA |
| 558 | rfaetim | Uhrzeit des RFA-Sitzungsendes | DRFA |
| 559 | afrcatid | Katalog-ID des Partnersystems | DRFA |
| 560 | afrproc | MRS-Prozessorname des Partners | DRFA |
| 561 | afruid | Benutzer-ID der AFR-Partneraufgabe | DRFA |
| 562 | afraccnr | Kontonummer der AFR-Partneraufgabezu | DRFA |
| 563 | afrtsn | TSN der AFR-Partneraufgabe | DRFA |
| 564 | trarec# | Anzahl übertragener Datensätze | DRFA |
| 565 | trabyte# | Anzahl übertragener Bytes | DRFA |
| 566 | rfascen | Jahrhundert der RFA-Verbindungsherstellung | DRFA |

| | | | |
|---|---|---|---|
| 567 | rfaecen | Jahrhundert des RFA-Sitzungsendes | DRFA |
| 568 | trasdat | Datum der Übertragungsanforderung | FTR0 |
| 569 | trastim | Uhrzeit der Übertragungsanforderung | FTR0 |
| 570 | traedat | Datum des Übertragungsendes | FTR0 |
| 571 | traetim | Uhrzeit des Übertragungsendes | FTR0 |
| 572 | trares | Übertragungsergebnis | FTR0 |
| 573 | folres | Ergebnis der Nachbearbeitung | FTR0 |
| 574 | partnam | Partnername | FTR0 |
| 575 | reqorig | Ursprung der Anforderung | FTR0 |
| 576 | reqident | Kennung der Anforderung | FTR0 |
| 577 | dskacc# | Anzahl der Plattenzugriffe | FTR0 |
| 578 | dskbyte# | Anzahl der Bytes auf Platte | FTR0 |
| 579 | netbyte# | Anzahl der Bytes im Netzwerk | FTR0 |
| 580 | splisdat | Datum des Spoolin-Starts | SPLI |
| 581 | splistim | Uhrzeit des Spoolin-Starts | SPLI |
| 582 | spliedat | Datum der Spoolin-Beendigung | SPLI |
| 583 | splietim | Uhrzeit der Spoolin-Beendigung | SPLI |
| 584 | #bsplfil | Anzahl an geschriebenen Bytes in die Spoolin-Datei | SPLI |
| 585 | #bdatfil | Anzahl an geschriebenen Bytes in andere Dateien | SPLI |
| 586 | sessdat | Datum des Sitzungsstarts | SRBS |
| 587 | sesstim | Uhrzeit des Sitzugsstarts | SRBS |
| 588 | sesedat | Datum der Sitzungsbeendigung | SRBS |
| 589 | sesetim | Uhrzeit der Sitzungsbeendigung | SRBS |
| 590 | rbatstat | Name der Remote-Batch-Station | SRBS |
| 591 | splicnt | Anzahl an Spoolin-Jobs | SRBS |

| | | | |
|---|---|---|---|
| 592 | consdat | Datum der Verbindung | BCA4 |
| 593 | constim | Uhrzeit der Verbindung | BCA4 |
| 594 | conedat | Datum der Verbindungsbeendigung | BCA4 |
| 595 | conetim | Uhrzeit der Verbindungsbeendigung | BCA4 |
| 596 | contim | Dauer der Verbindung | BCA4 |
| 597 | recvbyt# | Anzahl an empfangenen Bytes | BCA4 |
| 598 | sendbyt# | Anzahl an gesendeten Bytes | BCA4 |
| 599 | parproc# | Partner Prozessor Nummer | BCA4 |
| 600 | parreg | Partner Region Nummer | BCA4 |
| 601 | parappl | Partner Anwendungsname | BCA4 |
| 602 | parlan | Partner LAN-Adresse | BCA4 |
| 603 | paraddr | Partner Internet-Adresse | BCA4 |
| 604 | lparnam | Lokaler Name für den Partner | BCA4 |
| 605 | rfassea | Kennzeichen Jahreszeit für RFA-Verbindungsaufbau | DRFA |
| 606 | rfaesea | Kennzeichen Jahreszeit für RFA-Sitzungsende | DRFA |
| 672 | initproc | Initiator | BCA4 |
| 673 | profile | Profil | BCA4 |
| 674 | disact | Aktion, die die Trennung verursacht | BCA4 |
| 675 | sysrea | Systemgrund | BCA4 |
| 676 | userrea | Benutzergrund | BCA4 |
| 677 | asgdat | Datum der Gerätezuordnung | VACD |
| 678 | asgtim | Uhrzeit der Gerätezuordnung | VACD |
| 679 | asgcen | Jahrhundert der Gerätezuordnung | VACD |
| 680 | asgsea | Jahreszeit der Gerätezuordnung | VACD |
| 681 | errorcod<x> | Fehlercode | DRFA<STx> |
| 682 | tfilenam | Name der übertragenen Datei | FTR0 |
| 683 | libmemt | Typ des Bibliothekseintrags | FTR0 |

| | | | |
|---|---|---|---|
| 684 | libmemvr | Version des Bibliothekseintrags | FTR0 |
| 685 | libmemva | Variante des Bibliothekseintrags | FTR0 |
| 686 | libmemna | Name des Bibliothekseintrags | FTR0 |
| 687 | #locins | Anzahl verwendeter lokaler Anweisungen | FTR0 |
| 688 | cenreq | Jahrhundert der Übertragungsanforderung | FTR0 |
| 689 | cenend | Jahrhundert des Übertragungsendes | FTR0 |
| 690 | shortmn | Geräte-mn | SPLI |
| 691 | #crin | Anzahl eingelesener Karten | SPLI |
| 692 | #brin | Anzahl eingelesener Bytes | SPLI, SRBS |
| 693 | #rrin | Anzahl eingelesener Datensätze | SPLI, SRBS |
| 694 | fdiskvsn | Disketten-Volumenseriennummer (Floppy Disk) | SPLI |
| 695 | splnrbst | Spool-Name der RB-Station | SPLI |

# 4 Software-Produkt CLIP

Das Software-Produkt CLIP stellt in BS2000 Dienste zur Integration von sicherheitsrelevante Meldungen und Ereignisse aus dem BS2000-System in eine SIEM-Umgebung bereit.

CLIP ist ein nachladbares Subsystem in BS2000, Teil des Pakets BS2000 OS DX und auf aktuellen BS2000-Servern einsetzbar.

Das Subsystem besteht aus einer **privilegierten (TPR)** Komponente und einer **nicht privilegierten (TU)** Komponente. Die TU-Komponente wird beim Start des Subsystems durch das Job Management System (JMS) geladen, während die TPR-Komponente vom Dynamic Subsystem Management (DSSM) verwaltet wird.

Zum Ablauf des Programms wird im Subsystem CLIP unter der Kennung TSOS automatisch eine Batch-Task vom Typ TP mit dem Jobnamen CLIP gestartet. Diese Task arbeitet im Hintergrund als Daemon.

Hauptaufgaben der TPR-Komponente:

- Vorbereitung der Ausführung der TU-Komponente,
- Aufbau und Verwaltung einer FITC-Verbindung mit der TU-Komponente,
- Entgegennahme von Schnittstellenaufrufen privilegierter Tasks und deren Übergabe in den nicht privilegierten Adressraum,
- Kommunikation mit dem Operator über Konsolenmeldungen.

Hauptaufgaben der TU-Komponente:

- Kommunikation mit dem CLIP-Subsystem (TPR) und Entgegennahme der von dort übermittelten Nachrichten,
- Analyse und Aufbereitung (Parsing) der Nachrichten,
- Übertragung der aufbereiteten Nachrichten an einen Syslog-Server, wie zum Beispiel einen rSyslog-Server**.**

> ¡ Die zum Betrieb notwendigen aktuellen Versions- und Korrekturstände der Produkte und Komponenten finden Sie im in der aktuellen Freigabemitteilung zu BS2000 OS DX.

## 4.1 Produktstruktur von CLIP

Das Software-Produkt CLIP besteht aus der Liefereinheit CLIP.

Die Liefereinheit CLIP enthält die folgenden Bestandteile:

| Datei | Inhalt |
|---|---|
| SYSDAT.CLIP.<ver> | CLIP-Konfigurationsdatei |
| SYSENT.CLIP.<ver> | ENTER-Job für CLIP User Task. Dieser Job wird nur von CLIP intern verwendet |
| SYSPRG.CLIP.<ver> | Startprogramm für CLIP. Dieses Programm wird nur von CLIP intern verwendet. |
| SYSLNK.CLIP.<ver> | Ladebibliothek für /390-Server |
| SKMLNK.CLIP.<ver> | Ladebibliothek für x86-Server |
| SYSMES.CLIP.<ver> | Meldungsdatei |
| SYSSSC.CLIP.<ver> | Subsystem-Deklaration |
| SYSSII.CLIP.<ver> | IMON-Installationsinformation |
| SYSSPR.CLIP.<ver> | Kompilierte SDF-P-Prozedur zum Start des CLIP-TU-Programms. Die Prozedur wird nur von CLIP intern verwendet |

## 4.2 CLIP installieren und konfigurieren

Das Software-Produkt CLIP wird mit dem Installationsmonitors IMON installiert. Das genaue Vorgehen zur Installation ist in der aktuellen Freigabemitteilung zu BS2000 OS DX beschrieben.

Mit CLIP wird eine Konfigurationsdatei `SYSDAT.CLIP.<ver>` zur Konfiguration von CLIP geliefert.

Änderungen in der Konfigurationsdatei werden erst bei Neustart des CLIP-Subsystems wirksam. Die Einstellungen der Konfigurationsdatei werden in Abschnitt Konfiguration von CLIP beschrieben.

### 4.2.1 Betriebsnotwendige Ressourcen

CLIP benötigt zum Betrieb eine Batch-Task, die beim Start des Subsystems CLIP unter Kennung TSOS automatisch erzeugt wird.

Die Batch-Task wird in der Default-Jobklasse (für Batch unter Kennung TSOS) ohne Zeitbegrenzung gestartet. Die Task hat den Jobnamen `CLIP`.

### 4.2.2 Software-Anforderungen

Das Subsystem CLIP setzt voraus:

- BS2000 OS DX ab V1.0B
- Für den Support von SAT (Security Audit Trail) ist das Produkt SECOS im Einsatz und die Protokollierungskomponente SAT konfiguriert.
- Für den Support von ACCOUNTING Daten ist das BS2000 Abrechnungssystem eingeschaltet und konfiguriert.

### 4.2.3 Konfiguration von CLIP

Mit CLIP wird eine Konfigurationsdatei SYSDAT.CLIP.<ver> geliefert und mit dem Subsystem CLIP installiert. Diese ist für die jeweilige Konfiguration anzupassen. Änderungen der Konfiguration werden erst bei Neustart des Subsystems CLIP wirksam.

Beim Laden des Subsystems CLIP wird die Konfigurationsdatei gelesen und ausgewertet. Bei Fehlern in der Konfigurationsdatei wird der Ladevorgang fortgesetzt und die Standardwerte werden gesetzt.

Ausgenommen davon sind die syntaktisch fehlerhafte Angabe der IP-Adresse, oder eine nicht erreichbare IP-Adresse. In diesen Fällen ist kein sinnvoller Betrieb von CLIP möglich und der Subsystem-Start wird mit Fehler beendet.

- Bei syntaktisch fehlerhafter Angabe der IP-Adresse wird die Meldung GLP1020 an Konsole ausgegeben und das Subsystem CLIP beendet:

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

- Ist die konfigurierte IP-Adresse nicht erreichbar, wird das Subsystem CLIP nach Ablauf eines Timeout beendet.

**Original-Konfigurationsdatei**

Die Konfigurationsdatei SYSDAT.CLIP.<ver> wird als Template mit folgendem Inhalt ausgeliefert:

```
**********************************************************************
*                                                                    *
* 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 der Konfigurationsdatei:**

- Mit '*' beginnende Zeilen werden als Kommentarzeilen interpretiert.
- Einige Parameter sind mit Standardwerten vor belegt und müssen nicht spezifiziert werden. Der einzige obligatorische Parameter ist die Serveradresse (LOGSERVER), die vom Systemadministrator angegeben werden muss.
- Die Parameter werden unabhängig von ihrer Reihenfolge interpretiert.

- Die Parameter und ihre Werte werden ohne Unterscheidung von Groß- und Kleinschreibung behandelt und intern auf Großschreibung umgestellt.
- Zusammengehörige Parameter müssen in der gleichen Zeile angegeben werden, getrennt durch mindestens ein Leerzeichen.
- Alles, was nach dem letzten erforderlichen Parameter in einer Zeile erscheint und durch mindestens ein weiteres Leerzeichen getrennt ist, wird als Kommentar behandelt.

> ¡ Das json-Format für die Basis-Parameter der Konfigurationsdatei wird nur aus Kompatibilitätsgründen letztmalig unterstützt.

**Beschreibung der Basis-Parameter**

- "LOGSERVER" (obligatorisch)
  Mit diesem Parameter wird der Syslog-Server angegeben, an den die Meldungen gesendet werden. Der Wert kann eine IPv4/IPv6-Adresse oder ein Fully Qualified Domain Name (FQDN) sein.
  - IPv4: Muss dem Format xxx.xxx.xxx.xxx entsprechen (z. B. 192.168.1.99), wobei jedes Segment eine Zahl zwischen 0 und 255 ist.
  - IPv6: Sowohl vollständige als auch verkürzte Notationen sind zulässig (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334 und 2001:db8:85a3::8a2e:370:7334).
  - Wenn ein ungültiger Wert angegeben wird, erzeugt das CLIP-Programm eine Fehlermeldung und beendet sich, da eine gültige Serverkonfiguration erforderlich ist.
- "PORT"
  Der Parameter „PORT“ bezeichnet den bei der Kommunikation mit dem externen Syslog-Server zu verwendenden Port. Dieser Port muss ein gültiger offener Port im Bereich 1 – 65535 auf dem Syslog-Server sein, der für den BS2000-Server freigeschaltet ist. Der Parameter ist mit dem Standard-Port für Syslog-Datenverkehr (Port 514) vor belegt (auskommentiert).
- "PROTOCOL"
  Der Parameter "PROTOCOL" legt das Datenübertragungsprotokoll zwischen dem BS2000-Rechner und dem Syslog-Server fest. Aktuell wird nur das TCP-Protokoll unterstützt. Wird ein falscher Wert eingetragen oder der Parameter nicht angegeben, gilt der Standardwert „TCP“.
- "HOSTNAME"
  Der Parameter „HOSTNAME“ ist optional, da CLIP ihn bei fehlender Angabe automatisch ermittelt. Der Parameter definiert den Namen des BS2000-Systems und dient der Identifikation des BS2000-Systems beim Versenden von Ereignissen an den Syslog-Server. Der Parameter unterstützt alphanumerische Zeichen.
- "TIMEOUT"
  Der Parameter „TIMEOUT“ ist optional und gibt an, wie lange CLIP im Falle eines Verbindungsabbruches versucht, die Verbindung wiederherzustellen. Der Wert wird in Sekunden angeben und der Standardwert beträgt 30 Sekunden. Wenn nach dieser Zeitperiode die Wiederherstellung der Verbindung nicht erfolgreich war, wird das CLIP Subsystem beendet und muss bei Bedarf manuell neu gestartet werden.
- "OVERFLOW"
  Der Parameter „OVERFLOW“ ist optional und gibt an, ob CLIP Nachrichten wegwerfen soll, falls der Puffer bei einem Verbindungsabbruch vollläuft. Bei einem Wert von 0 (Standardwert) wird das Subsystem in diesem Fall beendet. Wird der Wert auf 1 gesetzt, werden die jeweils ältesten Nachrichten aus dem Puffer überschrieben. In beiden Fällen werden die Nachrichten im Puffer gesendet, sobald die Verbindung wiederhergestellt werden kann. Ob das Subsystem beendet wird (und die Nachrichten damit gelöscht werden), hängt dann lediglich vom TIMEOUT-Wert ab.

**Beschreibung der Parameter für die Filterfunktionen**

Zur Verbesserung der Performance, wie auch um die SIEM-Umgebung nur mit den Informationen zu beliefern, die aus Sicht des jeweiligen Anwenders sinnvoll sind, bietet CLIP eine Filterfunktion an. Die Filterfunktion wird sowohl für SATLOG- als aus auch für ACCOUNTING-Ereignisse angeboten und ist unabhängig einstellbar.

*Filterfunktion für SATLOG-Ereignisse:*

- "SATT MODE"
  Stellt ein, ob die in dieser Konfigurationsdatei aufgelisteten SATLOG-Ereignisse nicht ("BLOCK") oder ausschließlich ("ACCEPT") an den Syslog-Server weitergeleitet werden. Wird dieser Parameter nicht angegeben oder ein falscher Wert eingetragen, gilt aus Kompatibilitätsgründen automatisch der Wert "BLOCK".
  - SATT MODE BLOCK (Standardeinstellung): alle SATLOG-Ereignisse werden an den Syslog-Server weitergeleitet. Nur die in dieser Konfigurationsdatei aufgelisteten SATLOG-Ereignisse werden ausgefiltert und nicht an den Syslog-Server weitergeleitet.
  - SATT MODE ACCEPT: die SATLOG-Ereignisse werden ausgefiltert und nicht an den Syslog-Server weitergeleitet. Nur in dieser Konfigurationsdatei definierte SATLOG-Ereignisse werden explizit ausgewählt und an den Syslog-Server weitergeleitet.
- "SATT <eventid> <result>"
  Fügt das Ereignis <eventid> der durch "SATT MODE" definierten Liste in Abhängigkeit des Ergebnisses <result> hinzu. Interpretiert wird das Ereignis <result> im Erfolgsfall ("SUCC"), im Fehlerfall ("FAIL") oder in beiden Fällen ("BOTH"). Eine Übersicht der SAT Events ist im SECOS Handbuch im Abschnitt "SAT - Protokollierung und Auswertung sicherheitsrelevanter Ereignisse" zu finden.

*Filterfunktion für ACCOUNTING-Ereignisse:*

- "ACCT MODE"
  Stellt ein, ob die in dieser Konfigurationsdatei aufgelisteten ACCOUNTING-Ereignisse nicht ("BLOCK") oder ausschließlich ("ACCEPT") an den Syslog-Server weitergeleitet werden. Wird dieser Parameter nicht angegeben oder ein falscher Wert eingetragen, wird automatisch der Wert "BLOCK" angenommen.
  - ACCT MODE BLOCK (Standardeinstellung): alle ACCOUNTING-Ereignisse werden an den Syslog-Server weitergeleitet. Nur die in dieser Konfigurationsdatei aufgelisteten ACCOUNTING-Ereignisse werden ausgefiltert und nicht an den Syslog-Server weitergeleitet.
  - ACCT MODE ACCEPT: die ACCOUNTING-Ereignisse werden ausgefiltert und nicht an den Syslog-Server weitergeleitet. Nur in dieser Konfigurationsdatei definierte ACCOUNTING-Ereignisse werden explizit ausgewählt und an den Syslog-Server weitergeleitet.
- "ACCT <recordtype>"
  Fügt den Abrechnungssatz <recordtype> der durch "ACCT MODE" definierten Liste hinzu. Hierbei wird jeder Abrechnungssatz des angegebenen Typs beachtet. Im Abschnitt "Accounting-Logs" sind alle Ereignistypen aufgelistet.

**Beispielkonfiguration für die Filterfunktion:**

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

In diesem Beispiel wurde der BLOCK-Modus für SATLOG-Ereignisse eingeschalten. In den darauffolgenden drei Einträgen werden folgende Ereignisse ausgefiltert und damit **nicht** an den Syslog-Server weitergeleitet:

- Das Ereignis "JED" wird nur im Fehlerfall weitergeleitet
- Das Ereignis "UCK" wird ebenfalls nur im Fehlerfall weitergeleitet
- Das Ereignis "FRS" wird sowohl im Erfolgsfall, als auch im Fehlerfall gefiltert - und wird damit in keinem Fall an den Syslog-Server weitergeleitet
- Alle anderen Ereignisse werden uneingeschränkt weitergeleitet

Würde der Modus stattdessen auf ACCEPT geschalten werden (SATT MODE ACCEPT), würden nur die Ereignisse JED und UCK (nur im Erfolgsfall) und das Ereignis FRS (in allen Fällen) weitergeleitet werden. Alle anderen Ereignisse würden dann nicht mehr beachtet werden.

Da für das ACCOUNTING nichts definiert wurde, wird automatisch ACCT MODE BLOCK gesetzt. Da die Block-Liste jedoch leer ist, werden keine ACCOUNTING-Sätze gefiltert, es werden alle an den Syslog-Server weitergeleitet.

## 4.3 CLIP starten

Nach der Installation von CLIP kann das Subsystem CLIP gestartet werden mit:

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

Das Subsystem wird nicht automatisch nach `SYSTEM READY` gestartet, sondern muss vom Systemverwalter oder in der `CMDFILE` gestartet werden.

Ein erfolgreicher Start von CLIP ist unter folgenden Voraussetzungen möglich:

- Alle benötigten Dateien sind installiert.
- Die Version von CLIP passt zur BS2000-Version.
- Die IP-Adresse und der Port des Syslog-Server sind in der Konfigurationsdatei korrekt definiert.

Der erfolgreiche Start des Subsystem CLIP wird an der Konsole über die Meldungen GLPLOAD und ESM0220 protokolliert und kann mit Kommando `/SHOW-SUBSYSTEM SUBSYSTEM-NAME=CLIP` überprüft werden.

### Subsystem-Update im laufenden Betrieb:

Im Falle eines Versionswechsel des Subsystems CLIP (z.B. Installation und Start einer neueren Version) während des laufenden Betriebs sind folgende Schritte notwendig:

- CLIP-Subsystem mit dem Befehl `STOP-SUBSYSTEM` anhalten.
- Die neue Version von CLIP auf dem System installieren.
- SAT-Protokollierung mit dem Kommando `/HOLD-SAT-LOGGING` vorübergehend anhalten.
- Abrechnungssystem mit dem Kommando `/STOP-ACCOUNTING` ausschalten.
- Subsystem CLIP mit dem Kommando `/START-SUBSYSTEM` starten.
- SAT-Protokollierung mit Kommando `/RESUME-SAT-LOGGING` fortsetzten.
- Abrechnungssystem mit `/START-ACCOUNTING` einschalten.

> ¡ Die oben angegebene Reihenfolge ist unbedingt einzuhalten. Ansonsten wird der Start des Subsystems CLIP mit der Konsolmeldung GLP1025 abgewiesen:
>
> `GLP1025 START-SUBSYSTEM CLIP IS CURRENTLY NOT POSSIBLE`

> ¡ Die Meldungsdatei `SYSMES.CLIP.210` wird erst nach dem nächsten Systemneustart aktualisiert.

## 4.4 CLIP beenden

Das Subsystem CLIP kann jederzeit beendet werden mit:

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

DSSM wartet automatisch, bis der letzte Aufruf an CLIP abgeschlossen ist.

Die Meldungsausgaben an der BS2000-Konsole beim Beenden des Subsystems CLIP:

```
%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 Diagnosehilfen

CLIP ist ein nachladbares von BS2000 entkoppeltes Subsystem.

Die von CLIP erzeugten Tasks haben den Jobnamen `CLIP` .

CLIP informiert über alle Warnungs- und Fehlermeldungen an der BS2000-Konsole.

CLIP-Logging-Informationen für den TPR- und TU-Teil von CLIP (z.B. zur Diagnose zu Verbindungsproblemen zum Syslog-Server) sind unter der Kennung TSOS zu finden. Die Größe dieser Dateien sollte im Normalbetrieb 100 PAM-Seiten pro CLIP-Sitzung nicht überschreiten.

Bei Problemen im Umfeld von CLIP sind folgende Unterlagen zur Diagnose bereitzustellen:

1. CLIP-Logging-Dateien, werden bei jedem Subsystem-Start neu angelegt:
   - SYSLOG.CLIP.TU.<yyyy-mm-dd.hhmmss> – für den Batch-Job
   - SYSLOG.CLIP.SUBS.<yyyy-mm-dd.hhmmss> – für das Subsystem CLIP
2. CONSLOG-Datei
3. ggf. Systemdump
4. ggf. Diagnose-Unterlagen vom Syslog-Server

# 5 CLIP-Architektur

CLIP als BS2000-Subsystem versorgt über das Syslog-Protokoll z.B. externe SIEM-Systeme bei der Auswertung, Konsolidierung und Speicherung von Ereignissen aus mehreren angeschlossenen BS2000-Systemen. Dafür muss das Subsystem CLIP auf jedem der zu überwachenden BS2000 Systeme aktiv und passend konfiguriert sein.

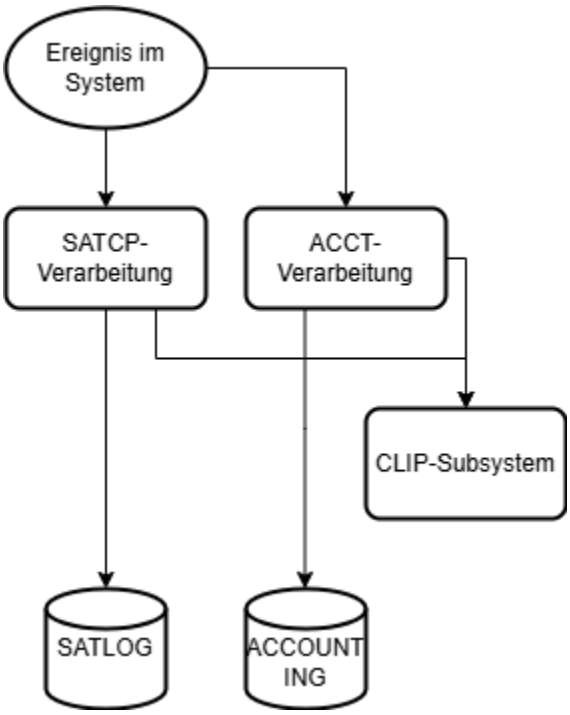
CLIP besteht aus zwei Teilen:

- TPR-Teil: das CLIP-Subsystem gesteuert über DSSM, zur zentralen Verarbeitung der BS2000-Ereignisse
- TU-Teil: der TU-Batch-Job zur Weiterleitung der BS2000-Ereignisse an einen externen Syslog-Server via Sockets

## TPR-Teil: CLIP-Subsystem

CLIP wird erstmals auf Basis BS2000 V21.0B bereitgestellt.

In der Abbildung wird schematisch die aktuelle CLIP-Einbindung für SAT und ACCOUNTING dargestellt.

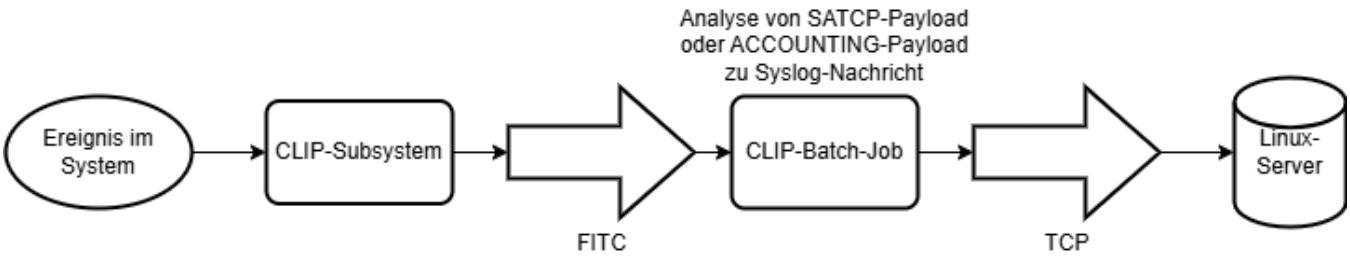



Der TPR-Teil von CLIP nimmt die SAT- und ACCOUNTING-Daten entgegen und überträgt sie an seinen TU-Teil.

## TU-Teil: CLIP-Batch-Job

Der CLIP-Batch-Job im TU-Teil baut eine TCP-Verbindung zum Syslog-Server auf, wartet auf Ereignisse vom TPR-Teil, analysiert diese und setzt sie in das Syslog-Format um. Nach erfolgreichem Parsing werden die Ereignisse via Socket-Schnittstelle an den in der CLIP-Konfigurationsdatei konfigurierten, externen Server gesendet. Auf dem externen Server muss an dem in CLIP konfigurierten Port ein Syslog daemon laufen. Dieser empfängt und filtert die empfangenen Daten und speichert sie in den Systemprotokollen des Servers.

In der Abbildung wird schematisch der aktuelle CLIP-Ablauf in TPR und TU am Beispiel von SAT und ACCOUNTING dargestellt.




Wenn die Verbindung zum Syslog-Server verloren geht, versucht der Batch-Job beim nächsten zu versendenden Ereignis, das mindestens eine Sekunde nach dem Verbindungsverlust auftritt, zyklisch die Verbindung wieder herzustellen. Dies wird solange wiederholt, bis es zu einem Timeout kommt oder der interne Pufferspeicher voll ist.

# 6 Anwendungsbeispiel: Rsyslog-Server

Im vorliegenden Kapitel wird als externer Syslog-Server beispielhaft rSyslog beschrieben.

rSyslog ist ein Open-Source-Softwaretool, das auf Linux-Computersystemen verwendet wird, um Protokollnachrichten über ein IP-Netzwerk weiterzuleiten. Es implementiert das grundlegende Syslog-Protokoll und erweitert es um inhaltsbasierte Filterung mit umfangreichen Funktionen. Das RSYSLOG-Dienstprogramm bietet verschiedene Funktionen wie Filterfähigkeiten, Warteschlangenverwaltung zur Behandlung von Offline-Ausgaben, Unterstützung verschiedener Modulausgaben, flexible Konfigurationsoptionen und die Verwendung von TCP für den Transport.

Rsyslog verwendet das BSD-Syslog-Standardprotokoll, wie in RFC 3164 definiert. Da der Text von RFC 3164 eher eine informative Beschreibung als eine Norm ist, wurden mehrere inkompatible Erweiterungen entwickelt. rSyslog unterstützt verschiedene dieser Erweiterungen (unter anderem auch RFC 5424) und erleichtert die Anpassung des Formats der weitergeleiteten Nachrichten (Quelle: https://en.wikipedia.org/wiki/Rsyslog).

## Installation

Installieren Sie das rSyslog-Paket auf einem externen Server bzw. VM (z.B. auf einer Application Unit (AU)) in Abhängigkeit des eingesetzten Betriebssystems.

### Starten des Dienstes:

Sie können rsyslog.service nach der Installation starten/aktivieren.

## Konfiguration

### Konfigurationsdatei

Die Konfiguration für rSyslog ist in der Datei /etc/rsyslog.conf gespeichert.

In /etc/rsyslog.conf sind folgende Einstellungen zum Empfang von CLIP-Ereignissen vorzunehmen:

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

Damit wird das TCP-Plugin für den Server aktiviert und der Standard-Port 514 zum Empfang der Syslog-Nachrichten geöffnet.

Für weitere Konfigurationsmöglichkeiten wird auf die Dokumentation von rSyslog verwiesen.

### Facility-Ebene

Alle von CLIP versendeten Nachrichten werden in rSyslog mit einer 'facility' von 1 (Nachrichten auf Benutzerebene) und einer 'severity' von 6 (informativ) konfiguriert.

# 7 Fachwörter

## ACCOUNTING

Systeminstanz zur Erfassung und Protokollierung von Abrechnungsdaten zu Systemressourcen wie CPU-Zeit, Speichernutzung oder I/O-Vorgängen im BS2000.

## Batch-Job

ENTER-Job

## DSSM (Dynamic Subsystem Management)

DSSM (Dynamic Subsystem Management) ist die zentrale Instanz in BS2000 für die dynamische Subsystemverwaltung.

## ENTER-Job

als Batch-Auftrag gestartete BS2000-Kommandofolge (ENTER-Datei).

## FQDN (Fully Qualified Domain Name)

Vollständiger Name einer Domäne

## JMS (Job Management System)

Job-Steuerung (Auftragssteuerung in BS2000)

## JSON (JavaScript Object Notation)

Dateiformat in lesbarer Textform zum Austausch strukturierter Daten zwischen Anwendungen.

## Linux

Familie von multitaskfähiger Mehrbenutzer-Betriebssystemen, die auf dem Linux-Kernel basieren.

## Parameterdatei

Auch Konfigurationsdatei. Dies ist eine Datei ($TSOS.SYSDAT.CLIP.<ver>), die die für das aktuelle Programm geltenden Parameter, Optionen, Einstellungen und Voreinstellungen definiert.

## Port

Ein Port ist eine zugewiesene Nummer zur eindeutigen Identifizierung eines Verbindungsendpunkts und zur Weiterleitung von Daten an einen bestimmten Dienst

## RFC (Request for Comment)

Publikation in einer Serie von den wichtigsten Stellen für technische Entwicklung und Normen setzenden Gremien für das Internet.

### rSyslog

Open-Source-Implementierung des Syslog-Protokolls auf Basis des BSD-Syslog-Protokolls ursprünglich spezifiziert in RFC 3164.

### SAT (Security Audit Trail)

SAT ist die Protokollierungskomponente von BS2000 für sicherheitsrelevante Ereignisse.

### SATCP (SAT Control Program)

Subsystem zum Überwachen von Ereignissen und Alarmen im Rahmen von SAT.

### SATUT

Dienstprogramm zur Auswertung und Bearbeitung der SATLOG-Dateien.

### SERSLOG

Softwarefehler-Protokollierung in BS2000.

### SIEM (Security Information and Event Management)

Systeme zum Sammeln, Überwachen und Analysieren von Sicherheitsdaten.

### Socket

Ein vom Betriebssystem bereitgestellter Kommunikations-Endpunkt für eine bidirektionale Kommunikation zwischen Anwendungen.

### Subsystem

Im Rahmen der dynamischen Subsystemverwaltung (DSSM) ist ein Subsystem eine Einheit, die eine Funktion ausführt und die automatisch und unabhängig geladen, gestartet und beendet werden kann, unter Berücksichtigung von Abhängigkeitsbeziehungen zu anderen Subsystemen. Ein Subsystem kann aus einer Reihe von Subsystemkomponenten bestehen.

### Syslog (System Logging Protocol)

Standard für die Nachrichtenprotokollierung in einem IP-Netzwerk.

### TCP (Transmission Control Protocol)

Eines der Hauptprotokolle der Internetprotokollfamilie. Das Protokoll ist
ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Transportprotokoll in Computernetzwerken.

### TCP/IP

Gebräuchliche Bezeichnung der Internetprotokollfamilie.

### TPR (Task privileged)

Privilegierte Teile des Betriebssystem BS2000 mit Ablauf im Systemadressraum.

## TSOS

Benutzerkennung für den Systemadministrator im BS2000 System.

## TU (Task unprivileged)

Nicht privilegierte Teile des Betriebssystem BS2000, z.B. auch Benutzerprogramme.

# 8 Literatur

Die Handbücher finden Sie im Internet unter http://bs2manuals.ts.fujitsu.com. Handbücher, die mit einer Bestellnummer angezeigt werden, können Sie in auch gedruckter Form bestellen.

**Betriebssystem BS2000 OS DX**
**Abrechnungssätze**
Benutzerhandbuch

**Betriebssystem BS2000 OS DX**
**DSSM**
Benutzerhandbuch

**DSSM/SSCM**
**Verwaltung von Subsystemen in BS2000**
Benutzerhandbuch

**openNet Server**
**SOCKETS**
Benutzerhandbuch

**SECOS**
Security Control System - Audit
Benutzerhandbuch