

Deutsch



FUJITSU Software BS2000

# SECOS V5.5

Security Control System - Beweissicherung

Benutzerhandbuch

Ausgabe März 2018

## **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 [manuals@ts.fujitsu.com](mailto:manuals@ts.fujitsu.com) senden.

## **Zertifizierte Dokumentation nach DIN EN ISO 9001:2008**

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 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH  
[www.cognitas.de](http://www.cognitas.de)

## **Copyright und Handelsmarken**

Copyright © 2018 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

---

# Inhalt

<b>1</b>	<b>Einleitung</b> . . . . .	<b>7</b>
<b>1.1</b>	<b>Zielgruppen des Handbuchs</b> . . . . .	<b>8</b>
<b>1.2</b>	<b>Readme-Datei</b> . . . . .	<b>9</b>
<b>1.3</b>	<b>Änderungen gegenüber der vorherigen Ausgabe</b> . . . . .	<b>10</b>
<b>1.4</b>	<b>Verwendete Metasprache</b> . . . . .	<b>11</b>
<b>2</b>	<b>SAT – Protokollierung und Auswertung sicherheitsrelevanter Ereignisse</b> . . . . .	<b>13</b>
<b>2.1</b>	<b>Rollen und Privilegien</b> . . . . .	<b>14</b>
<b>2.2</b>	<b>Subjekt, Objekt und Ereignis</b> . . . . .	<b>16</b>
<b>2.3</b>	<b>Steuern von Protokollierung und Auswertung</b> . . . . .	<b>19</b>
2.3.1	Auswahl sicherheitsrelevanter Ereignisse (Preselection) . . . . .	21
2.3.1.1	Auswahlverfahren . . . . .	21
2.3.1.2	Individuelle Steuerung der Auswahl . . . . .	26
2.3.2	Verfeinerung der Preselection durch den Filtermechanismus . . . . .	30
2.3.3	Verfeinern der Auswahl mit System-Exit Nr.110 . . . . .	32
2.3.4	Nachbearbeitung von SATLOG-Dateien (Postselection) . . . . .	33
2.3.5	Überwachung spezieller sicherheitsrelevanter Aktivitäten . . . . .	36
2.3.6	SAT-Alarm . . . . .	38
<b>2.4</b>	<b>Verwalten von SAT</b> . . . . .	<b>40</b>
2.4.1	SAT-Subsystem SATCP . . . . .	40
2.4.2	SAT-Parameter-Datei . . . . .	41
2.4.3	SAT-Protokolldateien (SATLOG) . . . . .	45
2.4.3.1	Schutz der SATLOG-Dateien . . . . .	45
2.4.3.2	Wechseln der SATLOG-Dateien . . . . .	46
2.4.3.3	Speicherplatzbedarf . . . . .	47
2.4.3.4	Aufbau der SATLOG-Dateien . . . . .	49
2.4.4	Überwachung durch SAT-spezifische Jobvariable . . . . .	53
2.4.5	SAT - Installation und Inbetriebnahme . . . . .	54

<b>2.5</b>	<b>SAT-Kommandos</b>	<b>56</b>
	Funktionelle Übersicht	56
	ADD-SAT-ALARM-CONDITIONS	
	Alarmbedingung definieren	60
	ADD-SAT-FILTER-CONDITIONS	
	Filterbedingung definieren	68
	CHANGE-SAT-FILE	
	SATLOG-Datei wechseln	76
	HOLD-SAT-LOGGING	
	Protokollierung anhalten	79
	MODIFY-SAT-ALARM-CONDITIONS	
	Alarmdefinition ändern	80
	MODIFY-SAT-FILTER-CONDITIONS	
	Filterdefinition ändern	93
	MODIFY-SAT-PRESELECTION	
	Auswahl treffen	106
	MODIFY-SAT-SUPPORT-PARAMETERS	
	Produktspezifische Aktivierung/Deaktivierung von Protokollierung und Alarmen	113
	REMOVE-SAT-ALARM-CONDITIONS	
	Alarmdefinition entfernen	116
	REMOVE-SAT-FILTER-CONDITIONS	
	Filterdefinition entfernen	117
	RESUME-SAT-LOGGING	
	Protokollierung fortsetzen	118
	SAVE-SAT-PARAMETERS	
	SATCP-Einstellungen speichern	120
	SHOW-SAT-ALARM-CONDITIONS	
	SAT-Alarmdefinitionen anzeigen	124
	SHOW-SAT-FILTER-CONDITIONS	
	SAT-Filterdefinitionen anzeigen	127
	SHOW-SAT-STATUS	
	SAT-Zustand anzeigen	131
	SHOW-SAT-SUPPORT-PARAMETERS	
	Einstellung der produktspezifischen Protokollierung und Alarmauslösung anzeigen	138
<b>2.6</b>	<b>SATUT – SATLOG-Dateien auswerten</b>	<b>140</b>
2.6.1	Arbeiten mit SATUT	140
2.6.2	Eingabedateien für SATUT	141
2.6.3	Arbeitsdateien im SATUT-Lauf	141
2.6.4	Ausgabe von SATUT	141
2.6.5	SATUT starten	144
	START-SATUT	
	Auswertung der SATLOG-Dateien einleiten	144

2.6.6	SATUT-Anweisungen . . . . .	146
	Funktionelle Übersicht . . . . .	146
	ADD-SELECTION-CONDITIONS	
	Auswahlbedingungen festlegen . . . . .	148
	END	
	Auswertung beenden . . . . .	155
	REMOVE-SELECTION-CONDITIONS	
	Auswahlbedingungen entfernen . . . . .	155
	SAVE-SELECTED-RECORDS	
	Ausgewählte Datensätze sichern . . . . .	156
	SELECT-INPUT-FILES	
	Eingabedateien festlegen . . . . .	158
	SELECT-RECORDS	
	Aufbereitungsbedingung festlegen . . . . .	163
	SHOW-REDUCTION-FILES-ORIGIN	
	Herkunft von replacement-files anzeigen . . . . .	164
	SHOW-SELECTED-RECORDS	
	Ausgewählte Datensätze ausdrucken . . . . .	167
	SHOW-SELECTION-CONDITIONS	
	Auswahlbedingungen anzeigen . . . . .	173
	SHOW-STATISTICS	
	SAT-Statistiken ausgeben . . . . .	174
	START-SELECTION	
	Auswertung einleiten . . . . .	186
2.6.7	Auswertungsbeispiel . . . . .	188
<b>2.7</b>	<b>Tabelle der Objekteignisse . . . . .</b>	<b>196</b>
<b>2.8</b>	<b>Tabellen der protokollierbaren Information je Objekteignis . . . . .</b>	<b>213</b>
<b>2.9</b>	<b>Tabelle der protokollierbaren Informationen (Feldnamen) . . . . .</b>	<b>279</b>
	<b>Fachwörter . . . . .</b>	<b>303</b>
	<b>Literatur . . . . .</b>	<b>317</b>
	<b>Stichwörter . . . . .</b>	<b>321</b>



---

# 1 Einleitung

SECOS (SEcurity CONTROL System) umfasst eine Produktpalette mit folgenden Bestandteilen: SRPM, GUARDS, GUARDDEF, GUARDCOO, SAT und SECOS-KRB. Diese Bestandteile stellen Verwaltungssysteme und Schnittstellen zur Verfügung, die für jeden einzelnen Benutzer einen individuellen Rahmen an Rechten und Pflichten definieren lassen. Sie spannen einen Bogen vom Einrichten, Verwalten und Löschen von Kennungen über das Arbeiten unter einer Kennung bis zur Überwachung, ob versucht wird, sich illegal Zugriff auf eine Kennung und deren Daten zu verschaffen.

- SRPM** (System Resources and Privileges Management). SRPM dient der Systemverwaltung (insbesondere dem Sicherheitsbeauftragten und der Benutzerverwaltung), um bereits bei der Einrichtung einer Kennung den Rahmen der Möglichkeiten für diese Kennung abzustecken. Die Kennung kann in ein Gruppenkonzept eingebunden und/oder ihr können besondere Privilegien zugewilligt werden. Auf diese Weise wird eine Benutzerstruktur errichtet, die Sicherheitsverstöße möglichst unwahrscheinlich bzw. die Quellen möglichst schnell lokalisierbar macht. Das Gruppenkonzept erlaubt es weiterhin, bestehende Projekt- und Organisationsformen im BS2000 nachzubilden.
- GUARDS** (Generally Usable Access control Administration System). GUARDS überwacht den Zugriff der Benutzer auf Dateien, Bibliotheken und weitere Objekte verschiedener Objektverwaltungen. Der Schutz durch GUARDS kann von der jeweiligen Objektverwaltung für alle und von jedem einzelnen Benutzer für seine eigenen Objekte verwendet werden. GUARDS bietet umfangreiche und flexible Möglichkeiten, Daten wirksam gegen unerlaubte Zugriffe zu schützen.
- GUARDDEF** (Default Protection, Standardschutz). GUARDDEF dient der Vergabe von Standardattributwerten für Dateien und Jobvariablen. Diese Werte können wahlweise für das Anlegen oder Modifizieren dieser Objekte vorgegeben werden. Die Einstellungen können von der Systemverwaltung (TSOS) jeweils pubset-weit und von jedem Benutzer für seine eigenen Objekte unter seiner Benutzerkennung vorgenommen werden. GUARDDEF nutzt GUARDS zur Ablage der Einstellungen.

- GUARDCOO** (Co-owner Protection, Miteigentümerschutz). Für Dateien und Jobvariablen kann die standardmäßig feste Eigentümer-Regelung im BS2000 (Eigentümer ist die Kennung, unter der das Objekt katalogisiert ist, TSOS ist Miteigentümer aller Dateien und Jobvariablen) verfeinert definiert werden. Dabei kann die Miteigentümerschaft für unterschiedliche Namensbereiche der Objekte sowohl der Benutzerkennung TSOS entzogen als auch anderen Benutzerkennungen oder den Inhabern bestimmter Privilegien gewährt werden. GUARDCOO nutzt GUARDS zur Ablage der Einstellungen.
- SAT** (Security Audit Trail). SAT ist die Protokollierungskomponente des BS2000 für sicherheitsrelevante Ereignisse. SAT kann eingesetzt werden, um Eindringversuche zu erkennen und um bei Verstößen gegen die Sicherheitsregelungen den Verursacher zu ermitteln. Dazu protokolliert SAT Ereignisse in SAT-Protokolldateien (SATLOG). In regelmäßigen Abständen müssen diese Dateien von Benutzern mit SAT-Privilegien ausgewertet werden. Hierzu dient das Auswertungsprogramm SATUT.
- Besonders sicherheitskritische Ereignisse können ohne Verzögerung mit Hilfe der SAT-Alarmfunktion überwacht werden. Die Alarmmeldung erscheint auf der Operator-Konsole, so dass entschieden werden kann, welche Maßnahmen ergriffen werden sollen.
- SECOS-KRB** SECOS-KRB ist die Schnittstelle zur Abwicklung der Kerberos-Authentisierung im BS2000.

Dieses Handbuch beschreibt die Komponente SAT (Security Audit Trail).

## 1.1 Zielgruppen des Handbuchs

Das Handbuch wendet sich vor allem an die Sicherheitsverwaltung und die Revision (Auswertung von Logging-Dateien). Es beschreibt die Funktionen der Komponente SAT des Produkts SECOS. Zum Verständnis des Handbuchs sind gute Kenntnisse der Sicherheitsfunktionen im Grundausbau des BS2000 erforderlich.

## 1.2 Readme-Datei

Ergänzungen gegenüber den Handbüchern sind gegebenenfalls in den Readme-Dateien zu den jeweiligen Produktversionen aufgeführt. Solche Readme-Dateien finden Sie sowohl auf der jeweils aktuellen SoftBooks-DVD als auch unter <http://manuals.ts.fujitsu.com> bei dem jeweiligen Produkt.

### *BS2000Ergänzende Produkt-Informationen*

Aktuelle Informationen, Versions-, Hardware-Abhängigkeiten und Hinweise für Installation und Einsatz einer Produktversion enthält die zugehörige Freigabemitteilung. Solche Freigabemitteilungen finden Sie unter <http://manuals.ts.fujitsu.com>.

## 1.3 Änderungen gegenüber der vorherigen Ausgabe

Die im Folgenden aufgeführten Änderungen beziehen nur auf die SECOS-Komponente SAT, die in diesem Handbuch beschrieben wird.

### Änderungen mit SECOS V5.4

Bei SELECT-INPUT-FILES können bis zu 100 Dateien angegeben werden. Entfallen sind SKP2-Dateien, Floppy-Disk, Lochkarte und Remote Batch.

### Änderungen mit SECOS V5.5

SECOS V5.5 wird unterstützt in Systemen mit BS2000 OSD/BC ab V10.0. Bestimmte Funktionen sind jedoch nur für Systeme mit BS2000 OSD/BC > V11.0A verfügbar. Auf solche Abhängigkeiten wird an den entsprechenden Stellen im Handbuch explizit hingewiesen.

Für POSIX-FILE -and-Directory werden 8 neue Ereignisse unterstützt:

- Verzeichnis via Deskriptor erzeugen (mkdirat)
- Link zu einer Datei via Deskriptor erzeugen (linkat)
- Dateizugriffsrechte via Deskriptor ändern (fchmodat)
- Datei via Deskriptor öffnen (openat)
- Dateiname via Deskriptor ändern (renameat)
- Symbolischen Verweis auf eine Datei via Deskriptor erzeugen (symlinkat)
- Datei oder Verzeichnis via Deskriptor löschen (unlinkat)
- Gruppe oder Besitzer einer Datei via Deskriptor ändern (fchownat)

Für die neuen Ereignisse können SAT-Information zusätzlich in den Feldern `atflag`, `dirdes1` und `dirdes2` auftreten. Das Feld `accmode` unterstützt zusätzlich `SEARCH` als Access mode.

### Allgemeine Hinweise

Die Bezeichnung des BS2000-Grundausbau lautet ab Version V10.0: BS2000 OSD/BC. Vorgängerversionen werden mit der bis dahin üblichen Bezeichnung BS2000/OSD-BC zitiert.

## 1.4 Verwendete Metasprache

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

- Literaturhinweise werden im Text in Kurztiteln angegeben. Der vollständige Titel jeder Druckschrift, auf die durch eine Nummer verwiesen wird, ist im Literaturverzeichnis hinter der entsprechenden Nummer aufgeführt.
- In den Beispielen sind Benutzereingaben und Systemausgaben in `Schreibmaschi-  
nenschrift` wiedergegeben.
- Besondere Hinweise auf Metasprache oder verwendete Symbole, die nur für einen Unterbestandteil gelten, finden sich zu Beginn des Kapitels zu diesem Unterbestandteil.
- Die Metasyntax für SDF-Kommandos und -Anweisungen, die Darstellung von Kommando-Returncodes und S-Variablen finden Sie im Handbuch „[BS2000 OSD/BC - Kommandos](#)“ [4].
- Die Metasyntax für Makros finden Sie im Handbuch „[BS2000 OSD/BC - Makroaufrufe an den Ablaufteil](#)“ [15].



Dieses Symbol steht zusammen mit dem Signalwort **ACHTUNG!** vor Warnhinweisen, die Sie im Interesse der System- und Betriebssicherheit unbedingt beachten müssen.



Dieses Symbol kennzeichnet wichtige Hinweise, die Sie unbedingt beachten sollten.



---

## 2 SAT – Protokollierung und Auswertung sicherheitsrelevanter Ereignisse

SAT (Security Audit Trail) unterstützt die Protokollierung sicherheitsrelevanter Ereignisse in eine geschützte SAT-Protokolldatei (SATLOG-Datei). Die SATLOG-Datei, erzeugt vom Subsystem SATCP, kann mit Hilfe des Auswerters SATUT analysiert werden, indem sinnvoll aufbereitete SAT-Protokolldateien und/oder Ergebnislisten erzeugt werden.

### Ziele der Protokollierung von Ereignissen

- Überblick über Zugriffe auf Objekte, Rückblick auf spezielle Verarbeitungsschritte und Aktionen bestimmter Benutzerkennungen, Gebrauch von Sicherheitsfunktionen
- Entdecken von unerlaubtem Eindringen in das System und (fremden) Anwendern, die Sicherheitsfunktionen umgangen haben
- Aufdecken bzw. Unterbinden des Gebrauchs von Rechten, die einem Benutzer nicht zugestanden sind
- Abschrecken vor dem Versuch, die Sicherheitsfunktionen zu umgehen
- Finden des Verursachers bei einem Verstoß gegen die Sicherheitsvorkehrungen, um so den Schaden gering zu halten
- Sofortiges Reagieren auf unerlaubte Systemeingriffe (Alarmfunktion)

### Protokollierbare Ereignisse

- Benutzung von Identifikations- und Authentisierungsmechanismen
- Zugriff auf Objekte (z.B. Eröffnen von Dateien, Programmstart)
- Anlegen und Löschen von Objekten
- Aktionen des Sicherheitsbeauftragten, der Systembedienung sowie der Systemverwaltung, die sicherheitsrelevant sind

### Protokollierte Daten

- Datum und Uhrzeit des Ereignisses
- eindeutige Identifikation des Ausführenden, bei Benutzung der Chipkarte auch die Chipkarten-Identifikation, bzw. die persönliche Benutzerkennung
- Erfolgs- oder Fehlerfall bei der Bearbeitung eines Verarbeitungsschrittes
- Name des bearbeiteten Objekts
- Beschreibung der Modifikation, die bei der Benutzerverwaltung oder im Rahmen der Systemsicherheit durchgeführt wurde

Eingriffe der Systembetreuung unterliegen nicht der SAT-Protokollierung, sie werden in der CONSLOG-Datei protokolliert. Diese können allerdings mit SATUT ausgewertet werden.

## 2.1 Rollen und Privilegien

Die Tätigkeitsbereiche Systemverwaltung und Systemüberwachung sollen aus Sicherheitsgründen nicht identisch sein. Deshalb werden mit der Privilegienverwaltung folgende Rollen eingeführt:

1. Der **Sicherheitsbeauftragte**, das ist die Benutzerkennung mit dem Privileg SECURITY-ADMINISTRATION. Er ist verantwortlich für
  - die Auswahl von Ereignissen (Preselection), die in den SATLOG-Dateien abgelegt werden (USER, EVENT, PRESELECTION-RULE, Festlegung der SAT-Support-Parameter)
  - die Verfügbarkeit von SAT-Funktionen (Anhalten und Fortsetzen der SAT-Protokollierung)
  - Definition von Ereignissen, die durch die SAT-Alarm-Funktion überwacht werden sollen
  - Definition von Filterbedingungen zur Verfeinerung der Preselection
  - die Zuweisung von Privilegien zur SAT-Verwaltung. Hierzu gehören die Systemprivilegien SAT-FILE-MANAGEMENT und SAT-FILE-EVALUATION

Das Privileg SECURITY-ADMINISTRATION ist bei Auslieferung der Benutzerkennung SYSPRIV fest zugeordnet. Die Zuordnung kann nur mit dem STARTUP-PARAMETER-SERVICE geändert werden.

2. Der **SAT-Datei-Verwalter**, das ist die Benutzerkennung mit dem Privileg SAT-FILE-MANAGEMENT. Er ist verantwortlich für
  - die Verwaltung von SAT-Dateien, einschließlich des Wechsels von SATLOG-Dateien
  - die Aufbereitung von Ereignissen (Postselection), die in den SATLOG-Dateien abgelegt sind, mit dem SAT-Auswertungsprogramm SATUT

Das Privileg SAT-FILE-MANAGEMENT ist bei Auslieferung der Benutzerkennung SYSAUDIT zugeordnet. Das Privileg kann vom Sicherheitsbeauftragten jeder anderen Benutzerkennung (außer sich selbst und der Kennung TSOS) überlassen werden.

3. Der **SAT-Datei-Auswerter**, das ist die Benutzerkennung mit dem Privileg SAT-FILE-EVALUATION. Er darf
  - SATLOG-Dateien auswerten, die vom SAT-Datei-Verwalter zur Verfügung gestellt wurden.

Das Privileg SAT-FILE-EVALUATION ist bei Auslieferung der Benutzerkennung SYSAUDIT zugeordnet. Der Sicherheitsbeauftragte kann das Privileg an mehrere beliebige Kennungen (außer an sich selbst) vergeben.

Die Möglichkeit, reduzierte SAT-Protokolldateien von mehreren Kennungen auswerten zu lassen, erlaubt es, nur bestimmte Informationen eines bestimmten Zusammenhangs (z.B. UTM, File-Transfer) vom jeweiligen Verwalter eines dieser Produkte auswerten zu lassen. Die Sicherheitsfunktionen von SAT bleiben weiterhin beim Sicherheitsbeauftragten und beim SAT-Datei-Verwalter.

## 2.2 Subjekt, Objekt und Ereignis

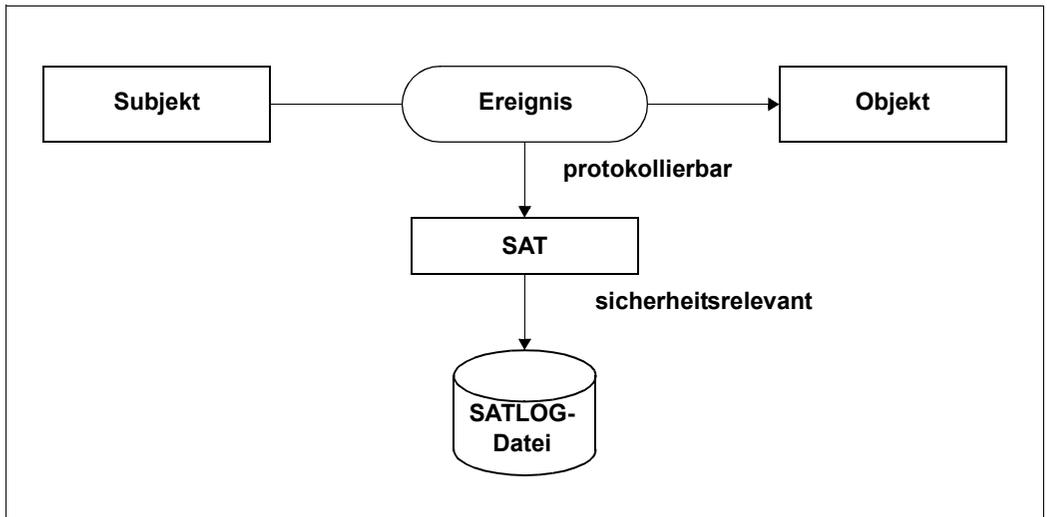


Bild 1: Subjekt, Objekt und Ereignis

Ein **Subjekt (USER)** ist ein Benutzer des DV-Systems, von dem eine Aktion wie lesen, schreiben, ausführen ausgehen kann. Er wird repräsentiert durch seine Benutzerkennung.

Ein **Objekt** ist ein passives Element eines DV-Systems, das Daten enthält oder aufnimmt und auf das eine Aktion wie lesen, schreiben, ausführen ausgeführt werden kann.

Objekte werden in SAT durch einen Objektnamen gekennzeichnet.

Objekte sind z.B.:

- Dateien (Objektname FILE)
- Jobs (JOB)
- Bibliotheken (PLAM)
- Benutzerkennungen (USERID)

Ein **Ereignis** ist die Aktion eines Subjekts auf ein Objekt. Das Ergebnis eines Ereignisses ist „erfolgreich ausgeführt (RESULT=SUCCESS)“ oder „nicht erfolgreich ausgeführt (RESULT=FAILURE)“.

Ereignisse sind z.B.:

- Datei öffnen
- Job starten
- Subsystem aktivieren
- Katalog exportieren

Ein **protokollierbares Ereignis (EVENT)** ist ein Ereignis aus der Liste der Ereignisse, die mit SAT protokolliert werden können. Sie werden gekennzeichnet durch einen dreistelligen Kurznamen, z.B. FMD für „Datei modifizieren“ im Objekt FILE.

Protokollierbare Ereignisse werden von den Systemkomponenten mit den zugehörigen Daten an SAT gemeldet.

Eine vollständige Liste der Objekte und ihrer protokollierbaren Ereignisse finden Sie im [Abschnitt „Tabelle der Objekt ereignisse“ auf Seite 196](#). Die Liste protokollierbarer Ereignisse und der zugehörigen Daten finden Sie im [Abschnitt „Tabellen der protokollierbaren Information je Objekt ereignis“ auf Seite 213](#).

Ein **sicherheitsrelevantes Ereignis** ist ein protokollierbares Ereignis, für das die Auswahlregeln, siehe [Abschnitt „Auswahlverfahren“ auf Seite 21](#), zutreffen. Ein protokollierbares Ereignis wird demnach erst sicherheitsrelevant, wenn die Verknüpfung der Audit-Attribute des Subjekts, des Ereignisses und des Objekts die Sicherheitsrelevanz anzeigen. Sicherheitsrelevante Ereignisse werden von SAT, ggf. nach Prüfung durch den System-Exit Nr. 110, in einer SATLOG-Datei gespeichert und können mit SATUT ausgewertet werden.

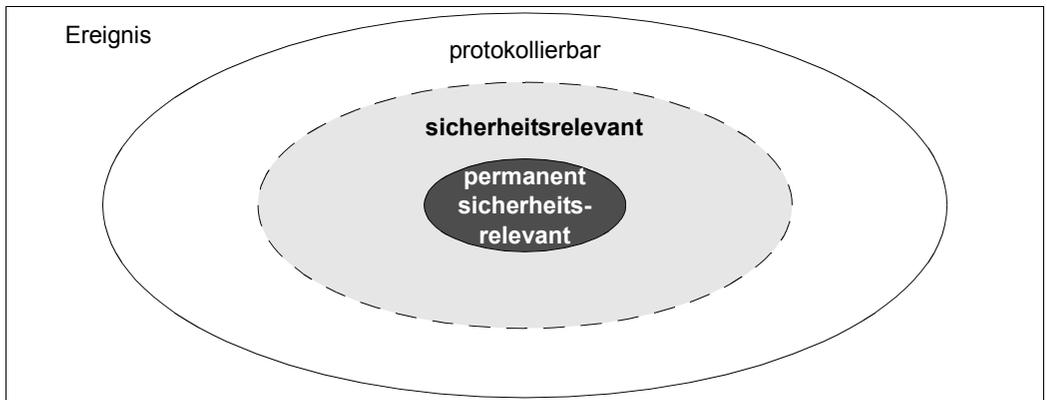


Bild 2: Ereignisarten

**Permanent sicherheitsrelevante Ereignisse** sind solche Ereignisse, die bei Einsatz von SECOS bzw. SAT unveränderbar sicherheitsrelevant sind. Für diese Ereignisse ist bereits eine Voreinstellung für das Audit-Attribut getroffen. Sie kann **nicht** verändert werden.

Permanent sicherheitsrelevante Ereignisse sind

- Aktionen des Sicherheitsbeauftragten und der SAT-Datei-Verwaltung (Benutzererkennung SYSAUDIT und Benutzerkennungen mit dem Privileg SECURITY-ADMINISTRATION oder SAT-FILE-MANAGEMENT) für die Objekte SAT, SAT-ALARM und SAT-FILTER
- Aktionen mit Privilegien (Vergabe / Entzug)

Die permanent sicherheitsrelevanten Ereignisse sind im [Abschnitt „Tabelle der Objekt ereignisse“ auf Seite 196](#) besonders gekennzeichnet.

Für alle anderen protokollierbaren Ereignisse entscheidet der Sicherheitsbeauftragte mit dem Kommando /MODIFY-SAT-PRESELECTION (**Preselection**), ob sie sicherheitsrelevant sind. Er kann einem Ereignis die Eigenschaft „sicherheitsrelevant“ sowohl vergeben als auch wieder entziehen.

Einige Ereignisse werden bei Einsatz von SECOS bzw. SAT neben den permanent sicherheitsrelevanten Ereignissen als sicherheitsrelevant erachtet. Für sie ist bereits per Voreinstellung ein Audit-Attribut festgelegt, das vom Sicherheitsbeauftragten allerdings verändert werden kann (Kommando /MODIFY-SAT-PRESELECTION).

Diese Ereignisse sind mit ihren Voreinstellungen in der „[Tabelle der Objekteignisse](#)“ auf [Seite 196](#) aufgeführt.

### **CONSLOG-Ereignisse**

CONSLOG- Meldungen werden vom Betriebssystem in eigenen Protokolldateien gesichert. Sie können nicht mit SAT zur Protokollierung ausgewählt werden.

Mit SATUT können auch CONSLOG-Protokolldateien in die Auswertung einbezogen werden. Dazu werden die CONSLOG- Meldungen in einen SATLOG-Satz umgewandelt. Der Kurzname für den Ereignis-Typ ist für CONSLOG-Ereignisse immer CLG. Der Inhalt des SATLOG-Satzes hängt davon ab, welcher Typ von CONSLOG- Meldung in einen SATLOG-Satz umgewandelt wurde (siehe [Seite 221](#)).

## 2.3 Steuern von Protokollierung und Auswertung

SAT bietet folgende optionale Steuerfunktionen, um die anfallende Datenmenge anlagen-spezifisch zu reduzieren und die Auswertungen zielgerecht durchführen zu können:

### 1. **SAT-Support-Einstellung**

Diese mit /MODIFY-SAT-SUPPORT-PARAMETERS festgelegte Einstellung ermöglicht es, von bestimmten Produkten ausgelöste Ereignisse für die Protokollierung (und Alarmierung) zu aktivieren oder zu deaktivieren. Derzeit ist diese produktspezifische Festlegung nur für Ereignisse des Produkts POSIX möglich.

- Ist der SAT-Support für ein Produkt deaktiviert, so werden alle Ereignisse dieses Produkts nicht mehr protokolliert (und für sie prinzipiell auch kein SAT-Alarm ausgelöst). Das heißt, die nachfolgenden Auswahlsschritte 2. - 5. haben keine Auswirkungen auf die Protokollierung dieser Ereignisse.
- Ist der SAT-Support für ein Produkt aktiviert, so sind für dessen Ereignisse die nachfolgenden Auswahlsschritte 2. - 5. uneingeschränkt wirksam.

2. **Preselection** – das ist die Vorabauswahl sicherheitsrelevanter Ereignisse in SATCP, um die zu protokollierende Ereignismenge klein zu halten

3. einen Filtermechanismus zur verfeinerten Vorauswahl

4. einen System-Exit, mit dem Sonderfälle gezielt bearbeitet werden können

5. **Postselection** – das ist die Nachbearbeitung der gespeicherten Daten mit dem Auswerteprogramm SATUT zur gezielten Auswertung und Archivierung sicherheitsrelevanter Ereignisse.

Die Ausgabe dieser Auswertung kann entweder in replacement-files oder in analysis-files erfolgen. Dabei dienen replacement-files im wesentlichen der **Archivierung** sicherheitsrelevanter Informationen aus den Eingabedateien und können diese somit ersetzen. Dagegen sind analysis-files hauptsächlich zur dezentralen **Analyse** sicherheitsrelevanter SATLOG-Sätze vorgesehen. Beide Dateitypen können in einem weiteren Auswertungslauf als Eingabedateien verwendet werden.

Zusätzlich können aufbereitete Datensätze in Arbeitsdateien (0 - 9) zwischengespeichert werden, um noch im selben Aufbereitungslauf weiterverarbeitet zu werden.

Das nachfolgende Bild zeigt das Zusammenspiel der Steuerfunktionen 2. - 5. bei der Reduzierung der möglichen Datenmenge.

Ein „event“ symbolisiert hier ein protokollierbares Ereignis, das abhängig von den vorgegebenen Auswahl-Kriterien und -Regeln von SAT protokolliert und ausgewertet wird.

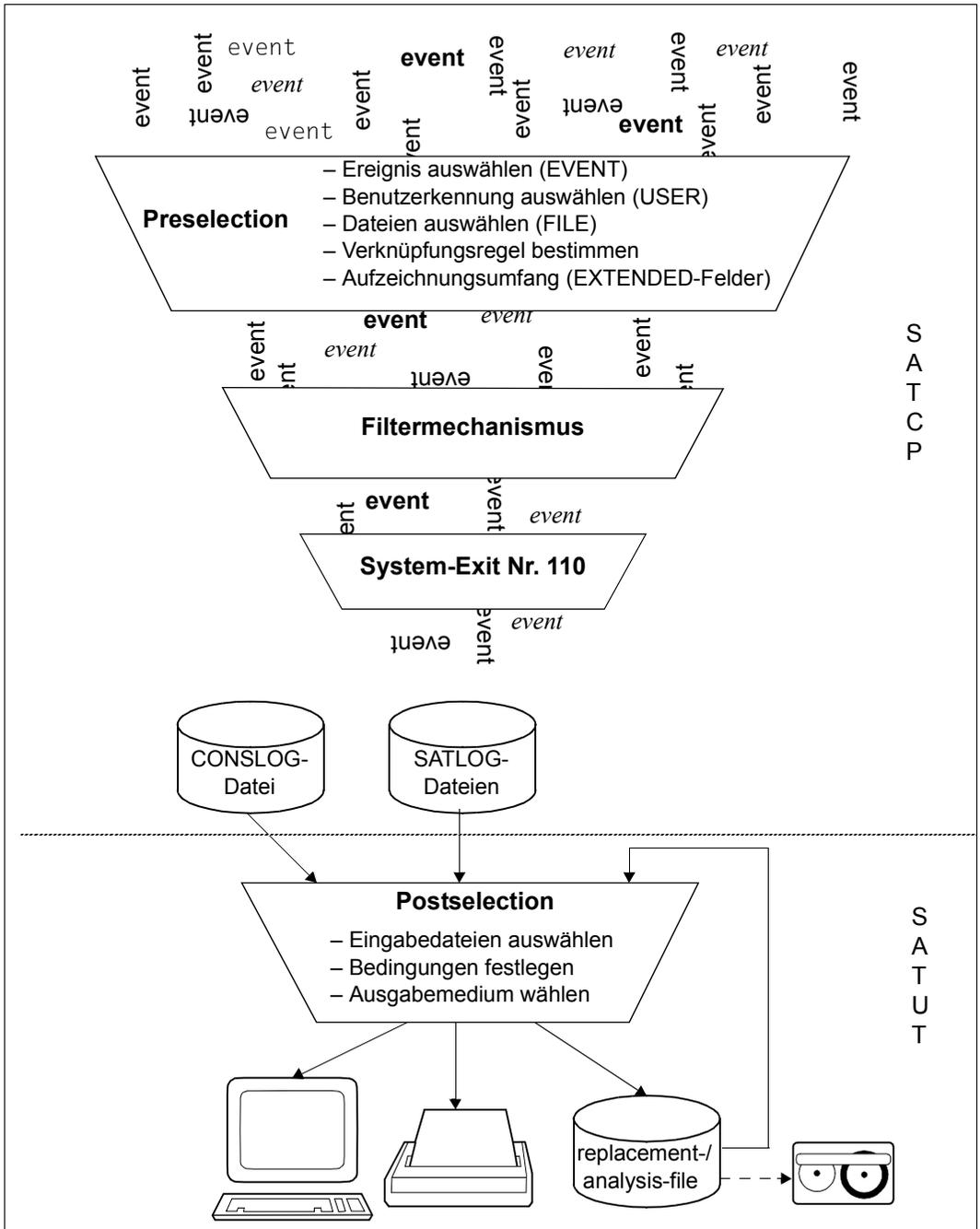


Bild 3: Steuerfunktionen von SAT

## 2.3.1 Auswahl sicherheitsrelevanter Ereignisse (Preselection)

Die Auswahl sicherheitsrelevanter Ereignisse erfolgt nach folgendem Auswahlverfahren durch den Sicherheitsbeauftragten.

### 2.3.1.1 Auswahlverfahren

Mit Ausnahme der permanent sicherheitsrelevanten Ereignisse legt der Sicherheitsbeauftragte fest, welche Ereignisse sicherheitsrelevant sind. Wenn ein Rechner nach dem Sicherheitsstandard F2/Q3 betrieben werden soll, muss der Sicherheitsbeauftragte keine Festlegungen vornehmen, da die System-Voreinstellung (siehe [Abschnitt „Tabelle der Objekt ereignisse“ auf Seite 196](#)) diesem Standard entspricht. Wenn der Sicherheitsbeauftragte jedoch andere Sicherheitskriterien voraussetzt, kann er Auswahlregeln für sicherheitsrelevante Ereignisse mit dem Kommando /MODIFY-SAT-PRESELECTION vorgeben.

Bestimmende Elemente bei der Auswahl eines sicherheitsrelevanten Ereignisses sind

- die Benutzerkennung (USER)
- das protokollierbare Ereignis (EVENT) und das Ereignis-Ergebnis (RESULT)
- die Benutzervorgaben für die besonderen Objekte Datei und Bibliothek (FILE) und das Ereignis-Ergebnis (RESULT)
- die Verknüpfungsregel für die obigen drei Elemente
- den Ausgabeumfang, mit dem festgelegt ist, ob \*EXTENDED-Felder aufgezeichnet werden (siehe [Abschnitt „Tabellen der protokollierbaren Information je Objekt ereignis“ auf Seite 213](#))

Mit dem Kommando SHOW-SAT-STATUS können sich der Sicherheitsbeauftragte und die SAT-Datei-Verwaltung die Auswahl anzeigen lassen.

### Benutzerkennung (USER)

Die Auswahl sicherheitsrelevanter Benutzerkennungen erfolgt durch den Sicherheitsbeauftragten durch Vorgabe eines Audit-Attributes für die Benutzerkennung mit dem SAT-Kommando /MODIFY-SAT-PRESELECTION, Operand USER-AUDITING.

Folgende Audit-Attribute können vergeben werden:

- |     |   |
|-----|---|
| OFF | Benutzerkennung ist nicht sicherheitsrelevant |
| ON  | Benutzerkennung ist sicherheitsrelevant       |

Das vergebene Audit-Attribut wird in den Benutzerkatalog eingetragen. Es ist sofort gültig und bleibt bis zur nächsten Änderung, auch in einer neuen Session, bestehen.

*Voreinstellung*

Beim ersten Einsatz von SAT haben alle Benutzerkennungen das Audit-Attribut ON; ihre protokollierbaren Ereignisse sind sicherheitsrelevant, bis der Sicherheitsbeauftragte das Audit-Attribut ändert.

Für neu eingerichtete Benutzerkennungen ist das Audit-Attribut ebenfalls ON. Ihre protokollierbaren Ereignisse sind sicherheitsrelevant, bis der Sicherheitsbeauftragte das Audit-Attribut ändert. Diese Voreinstellung kann mit dem Kommando /MODIFY-SAT-PRESELECTION geändert werden.

Für die Benutzerkennung SYSAUDIT und Kennungen mit den Privilegien SAT-FILE-MANAGEMENT oder SECURITY-ADMINISTRATION ist das Audit-Attribut ON und kann auch nicht geändert werden; protokollierbare Ereignisse dieser Benutzerkennungen sind immer sicherheitsrelevant.

**Ereignis (EVENT)**

Die Auswahl von Ereignissen erfolgt durch den Sicherheitsbeauftragten durch Vorgabe eines Audit-Attributes mit dem SAT-Kommando /MODIFY-SAT-PRESELECTION, Operand EVENT-AUDITING.

Folgende Audit-Attribute können für das Ereignis vergeben werden:

NONE	Ereignis ist nicht sicherheitsrelevant
SUCCESS	Ereignis ist bei erfolgreicher Ausführung (RESULT=SUCCESS) sicherheitsrelevant
FAILURE	Ereignis ist bei nicht erfolgreicher Ausführung (RESULT=FAILURE) sicherheitsrelevant
ALL	Ereignis ist sicherheitsrelevant

Audit-Attribute für Ereignisse werden in SAT vermerkt und sind in der laufenden Session nur bis zur nächsten Änderung oder bis zum SHUTDOWN gültig.

Sie können auch, zur Verwendung in späteren Sessions, in der SAT-Parameter-Datei gespeichert werden (siehe [Abschnitt „SAT-Parameter-Datei“ auf Seite 41](#)).

In der nächsten Session gelten die (alten oder geänderten) Einstellungen der SAT-Parameter-Datei.

*Voreinstellung*

Siehe [Abschnitt „Tabelle der Objekteignisse“ auf Seite 196](#).

Für permanent sicherheitsrelevante Ereignisse ist das Audit-Attribut obligatorisch ALL, es kann nicht geändert werden.

## Benutzervorgaben (FILE)

Für die besonderen Objekte Datei und Bibliothek erfolgt die Vergabe des Audit-Attributs mit Hilfe der DVS-Kommandos /CREATE-FILE bzw. /MODIFY-FILE-ATTRIBUTES durch

- den Dateibesitzer, wenn dieser durch den Gruppenverwalter oder den systemglobalen Benutzerverwalter dazu berechtigt wurde (Benutzerkatalog-Eintrag FILE-AUDIT=\*ALLOWED)
- den privilegierten Benutzer TSOS

Folgende Audit-Attribute können für Datei-Objekte vergeben werden:

NONE	Objekt ist nicht sicherheitsrelevant
SUCCESS	Objekt ist bei erfolgreicher Ereignis-Ausführung (RESULT=SUCCESS) sicherheitsrelevant
FAILURE	Objekt ist bei nicht erfolgreicher Ereignis-Ausführung (RESULT= FAILURE) sicherheitsrelevant
ALL	Objekt ist sicherheitsrelevant

Das vergebene Audit-Attribut wird in den Dateikatalog eingetragen. Es ist sofort gültig und bleibt bis zur nächsten Änderung, auch in einer neuen Session, bestehen.

### *Voreinstellung*

Die Datei-Objekte sind nicht sicherheitsrelevant (Audit-Attribut=NONE).

## Verknüpfungsregeln

Zur Verknüpfung der bestimmenden Elemente bei der Auswahl gibt es zwei Verknüpfungsregeln:

- INDEPENDENT-Regel
- FILES-BY-EVENTS-Regel

Die Verknüpfungsregel wird vom Sicherheitsbeauftragten mit dem Kommando /MODIFY-SAT-PRESELECTION, Operand PRESELECTION-RULE festgelegt.

Die Verknüpfungsregel wird in SAT vermerkt und ist zunächst nur bis zur nächsten Änderung oder bis zum SHUTDOWN gültig.

Sie kann auch, zur Verwendung in späteren Sessions, in der SAT-Parameter-Datei gespeichert werden (siehe [Abschnitt „SAT-Parameter-Datei“ auf Seite 41](#)).

In der nächsten Session gilt die (alte oder geänderte) Einstellung der SAT-Parameter-Datei.

### *Voreinstellung*

INDEPENDENT-Regel

Bei der **INDEPENDENT-Regel** werden die bestimmenden Elemente durch ein logisches ODER verknüpft. Ein Ereignis wird immer dann protokolliert, wenn wenigstens eines der drei bestimmenden Elemente sicherheitsrelevant ist.

Ein protokollierbares Ereignis ist demnach sicherheitsrelevant, wenn

- das Subjekt (die Benutzerkennung) sicherheitsrelevant ist  
d.h. das Audit-Attribut für die Benutzerkennung ist gesetzt (ON)

ODER

- das Ereignis (EVENT) sicherheitsrelevant ist  
d.h. die Kombination des Audit-Attributs von EVENT mit dem Ereignis-Ergebnis liefert die Anzeige „sicherheitsrelevant“ (siehe Tabelle).

ODER

- das Datei-Objekt (FILE) sicherheitsrelevant ist  
d.h. die Kombination des Audit-Attributs von FILE mit dem Ereignis-Ergebnis liefert die Anzeige „sicherheitsrelevant“ (siehe Tabelle).

Für Objekte, die nicht Datei-Objekte sind, spielt FILE keine Rolle, es gilt USER ODER EVENT

	<b>Audit-Attribut für EVENT oder FILE</b>			
	<b>NONE</b>	<b>SUCCESS</b>	<b>FAILURE</b>	<b>ALL</b>
<b>Ereignis erfolgreich ausgeführt RESULT=SUCCESS</b>	nicht sicherheits relevant	sicherheits relevant	nicht sicherheits relevant	sicherheits relevant
<b>Ereignis nicht erfolgreich ausgeführt RESULT=FAILURE</b>	nicht sicherheits relevant	nicht sicherheits relevant	sicherheits relevant	sicherheits relevant

Tabelle 1: Kombination der Audit-Attribute von EVENT und FILE mit dem Ereignis-Ergebnis

Bei der **FILES-BY-EVENTS-Regel** werden EVENT und FILE mit der UND-Logik verknüpft.

Ein protokollierbares Ereignis ist demnach sicherheitsrelevant, wenn

- das Subjekt (die Benutzererkennung) sicherheitsrelevant ist  
d.h. das Audit-Attribut für die Benutzererkennung ist gesetzt (ON)

ODER

- das Ereignis (EVENT) sicherheitsrelevant ist  
d.h. die Kombination des Audit-Attributs von EVENT mit dem Ereignis-Ergebnis liefert die Anzeige „sicherheitsrelevant“ (siehe Tabelle oben).

UND

- das Datei-Objekt (FILE) sicherheitsrelevant ist  
d.h. die Kombination des Audit-Attributs von FILE mit dem Ereignis-Ergebnis liefert die Anzeige „sicherheitsrelevant“ (siehe Tabelle oben).

Für Objekte, die nicht Datei-Objekte sind, spielt FILE keine Rolle, es gilt analog zur INDEPENDENT-Logik die Bedingung USER ODER EVENT

#### *Hinweis*

Die Gestaltung der Verknüpfungsregeln zeigt, dass auch bei Reduzierung der sicherheitsrelevanten Ereignismenge auf ein Minimum (siehe [Seite 29](#)) wenigstens **alle** protokollierbaren Ereignisse der Benutzererkennung SYSAUDIT und der Benutzerkennungen mit den Privilegien SAT-FILE-MANAGEMENT oder SECURITY-ADMINISTRATION (siehe [Seite 22](#)) sicherheitsrelevant sind und protokolliert werden.

### **Aufzeichnungsumfang**

\*EXTENDED-Felder sind Felder, die erweiterte Information zu einem Ereignis enthalten. Sie sind in den „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf [Seite 213ff](#) mit „E“ gekennzeichnet. Diese Felder werden nur aufgezeichnet, wenn der Sicherheitsbeauftragte die Aufzeichnung mit der Angabe LOGGING-QUANTITY=\*EXTENDED im Kommando /MODIFY-SAT-PRESELECTION erlaubt.

#### *Voreinstellung*

\*EXTENDED-Felder werden nicht aufgezeichnet.

### 2.3.1.2 Individuelle Steuerung der Auswahl

#### Voreinstellungen

Die Auswahl-Einstellungen von SAT bei erstem Einsatz bzw. ohne individuelle Steuerung sind:

- Benutzerkennung: Für bestehende Benutzerkennungen sind die Auswahl-Einstellungen entsprechend den Einträgen im Benutzerkatalog.  
Für neu eingerichtete Benutzerkennungen werden alle Ereignisse protokolliert
- Ereignis: Voreinstellung sicherheitsrelevanter Ereignisse (siehe [Abschnitt „Tabelle der Objekteignisse“ auf Seite 196](#))
- Datei-Objekt: entsprechend den Einträgen im Dateikatalog
- Verknüpfungsregel: INDEPENDENT-Regel
- Filter-Aktivierung: kein Filter aktiv
- Exit-Aktivierung: System-Exit Nr. 110 nicht aktiv
- Aufzeichnungsumfang: \*EXTENDED-Felder werden nicht aufgezeichnet

#### Auswahl für die laufende Session

Die Auswahl sicherheitsrelevanter Benutzerkennungen und Ereignisse sowie der Verknüpfungsregel und des Aufzeichnungsumfangs kann vom Sicherheitsbeauftragten mit dem Kommando /MODIFY-SAT-PRESELECTION getroffen werden, wenn SAT aktiv ist.

Wird SAT vom Sicherheitsbeauftragten mit dem Kommando /HOLD-SAT-LOGGING angehalten und im gleichen Systemlauf mit dem Kommando /RESUME-SAT-LOGGING wieder gestartet, gelten die gleichen Auswahl-Einstellungen wie vor dem Anhalten.

Ist SAT angehalten, kann die Auswahl sicherheitsrelevanter Ereignisse nicht verändert werden, das Kommando /MODIFY-SAT-PRESELECTION wird nicht ausgeführt.

#### Auswahl für Folgesessions

Der Sicherheitsbeauftragte kann die Sicherheitsrelevanz von Benutzerkennungen und Ereignissen sowie die Verknüpfungsregel auch für nachfolgende Sessions festlegen.

Einstellungen für Benutzerkennungen (USER) und Datei-Objekte (FILE) gelten automatisch in nachfolgenden Sessions, da sie im Benutzerkatalog bzw. im Dateikatalog hinterlegt sind. Für Ereignisse, die Voreinstellung für neue Benutzerkennungen, die Verknüpfungsregel und den Aufzeichnungsumfang müssen die Festlegungen explizit mit dem Kommando /SAVE-SAT-PARAMETERS in der SAT-Parameter-Datei gespeichert werden, um beim nächsten Systemstart wirksam zu werden.

## Hinweis zur Auswahl von Benutzerkennungen

Standardmäßig erhält jede **neue** Benutzerkennung das Audit-Attribut ON, d.h. alle von ihr ausgelösten Ereignisse werden automatisch protokolliert. Hält der Sicherheitsbeauftragte dies nicht für notwendig, kann er diese Voreinstellung modifizieren, so dass alle neuen Benutzerkennungen das Audit-Attribut OFF erhalten.

### *Beispiel*

Für alle neuen und alle schaltbaren Benutzerkennungen wird das Audit-Attribut auf OFF gesetzt (Schaltbare Benutzerkennungen sind alle Kennungen, außer SYSAUDIT und Kennungen mit dem Privileg SECURITY-ADMINISTRATION oder SAT-FILE-MANAGEMENT). Für die Benutzerkennungen <user1>, <user2>, <user3>, ... wird das Audit-Attribut auf ON gesetzt. Das bedeutet: alle Ereignisse, die von den Benutzerkennungen <user1>, <user2>, <user3>, ... ausgelöst werden, sind sicherheitsrelevant und werden protokolliert.

```
/modify-sat-preselection user-auditing=*default(new-user=*off)
/modify-sat-preselection user-auditing=*all-switchable(audit-switch=*off)
/modify-sat-preselection user-auditing=(<user1>,<user2>,<user3>,...)
```

Die Kennung TSOS und alle Benutzerkennungen, die ein von STD-PROCESSING abweichendes Privileg erhalten haben, sollten stets protokolliert werden. Die Kennungen des Sicherheitsbeauftragten, die Kennung SYSAUDIT und Kennungen mit dem Privileg SAT-FILE-MANAGEMENT werden immer protokolliert. Das Ausschalten der Protokollierung ist für diese Kennungen nicht möglich. Wird einer Benutzerkennung mit Audit-Attribut OFF das Privileg SECURITY-ADMINISTRATION (nur über Startup-Parameterservice) oder SAT-FILE-MANAGEMENT (Kommando /SET-PRIVILEGE) zugeteilt, dann wird ihr Audit-Attribut automatisch auf ON gesetzt.

## Hinweis zur Auswahl von Ereignissen

Individuelle Auswahlsteuerungen, die bereits bei STARTUP wirksam sein sollen, können entweder in der SAT-Parameter-Datei gespeichert werden oder sie müssen nach jeder Systemeinleitung erneut durch den Sicherheitsbeauftragten über das Kommando /MODIFY-SAT-PRESELECTION bekanntgegeben werden (z.B. in einem automatisch ablaufenden Batchauftrag).

*Beispiel*

Die Ereignisse „Programm laden/ausführen“ (XLD) und „Programm entladen“ (XUL) sollen unabhängig von ihrem Ergebnis zur Protokollierung ausgewählt werden. Das Ereignis „Userid hinzufügen“ (UAD) soll bei erfolgreicher Ausführung protokolliert werden, das Ereignis „Userid prüfen“ (UCK) bei nicht erfolgreicher Ausführung. Abweichend von der Voreinstellung im System hält der Sicherheitsbeauftragte UTM-Ereignisse (TRM) für nicht sicherheitsrelevant und möchte sie daher nicht protokollieren. Diese Einstellungen sollen auch in nachfolgenden Sessions gelten.

Zur Einstellung der Auswahl ist folgendes Kommando erforderlich:

```
/modify-sat-preselection event-auditing=(
    xld,
    xul,
    uad(audit-switch=*on(result=*success)),
    uck(audit-switch=*on(result=*failure)),
    trm(audit-switch=*off))
```

Damit diese Einstellung automatisch bei STARTUP wirksam ist, kann man das Kommando in einem Batch-Job ausführen, der bei jedem STARTUP abläuft. Es empfiehlt sich stattdessen jedoch, nach einmaliger Ausführung des Kommandos MODIFY-SAT-PRESELECTION die Einstellung in der SAT-Parameter-Datei zu speichern mit

```
/save-sat-parameters event-preselection=*current
```

## Minimierung der Anzahl protokollierter Ereignisse

Die Menge der protokollierten Ereignisse kann mit folgendem Kommando minimiert werden:

```
/modify-sat-preselection event-auditing=( -  
/ cep(audit-switch=*off),cip(audit-switch=*off),gad(audit-switch=*off), -  
/ gmd(audit-switch=*off),grm(audit-switch=*off),jbe(audit-switch=*off), -  
/ jde(audit-switch=*off),jfk(audit-switch=*off),jin(audit-switch=*off), -  
/ jvg(audit-switch=*off),jvm(audit-switch=*off),jvs(audit-switch=*off), -  
/ kea(audit-switch=*off),ked(audit-switch=*off),kpa(audit-switch=*off), -  
/ kpd(audit-switch=*off),kpm(audit-switch=*off),ktc(audit-switch=*off), -  
/ kxm(audit-switch=*off),mac(audit-switch=*off),psc(audit-switch=*off), -  
/ psd(audit-switch=*off),scr(audit-switch=*off),sct(audit-switch=*off), -  
/ sdl(audit-switch=*off),shd(audit-switch=*off),srm(audit-switch=*off), -  
/ srs(audit-switch=*off),tba(audit-switch=*off),tbd(audit-switch=*off), -  
/ tbe(audit-switch=*off),tbi(audit-switch=*off),tka(audit-switch=*off), -  
/ tkc(audit-switch=*off),tkp(audit-switch=*off),tkr(audit-switch=*off), -  
/ trm(audit-switch=*off),tvm(audit-switch=*off),twk(audit-switch=*off), -  
/ uad(audit-switch=*off),uck(audit-switch=*off),udm(audit-switch=*off), -  
/ uds(audit-switch=*off),uml(audit-switch=*off),ump(audit-switch=*off), -  
/ uop(audit-switch=*off),urm(audit-switch=*off),usl(audit-switch=*off), -  
/ uul(audit-switch=*off),uup(audit-switch=*off),uus(audit-switch=*off), -  
/ vda(audit-switch=*off),vdu(audit-switch=*off),vid(audit-switch=*off), -  
/ vip(audit-switch=*off))
```

Damit wird die Protokollierung für alle Ereignisse abgeschaltet, für die vom BS2000 bereits ein Audit-Attribut per Voreinstellung festgelegt ist, das aber verändert werden darf (siehe [Abschnitt „Tabelle der Objekteignisse“ auf Seite 196](#)).

## 2.3.2 Verfeinerung der Preselection durch den Filtermechanismus

Der Filtermechanismus erlaubt dem Sicherheitsbeauftragten eine Verfeinerung der Preselection und bietet damit die Möglichkeit, die Aufzeichnungsmenge detaillierter zu verringern.



### **ACHTUNG!**

Falls eine Aufzeichnung nach Sicherheitsstandard F2/Q3 gewünscht ist, dürfen keine Filter eingesetzt werden. Es muss die Standard-Preselection benutzt werden.

Es dürfen maximal 32 Filterbedingungen mit folgenden Angaben festgelegt werden:

- Ereignisse und Resultat
- Subjekte (USER-ID)
- Informationen (Felder und deren Inhalt).

Für Feldwerte, die zeichenweise darstellbar sind (z.B. <c-string>, <filename>), können Wildcards angegeben werden.

Diese Angaben können als Positivlisten (einzelne Aufzählungen) oder Negativlisten (\*ALL, außer einzelne Aufzählungen) erfolgen. Sie werden durch logisches UND miteinander zu einer Bedingung verknüpft.

Eine Filterbedingung trifft also dann auf einen Protokollsatz zu, wenn alle Teilangaben auf den Protokollsatz zutreffen.

Für jede Filterbedingung wird mit dem Operanden TRIGGER-ACTION der Kommandos /ADD-SAT-FILTER-CONDITIONS oder /MODIFY-SAT-FILTER-CONDITIONS eine Aktion festgelegt, die ausgeführt werden soll, wenn die Filterbedingung auf den Protokollsatz zutrifft.

Für TRIGGER-ACTION kann festgelegt werden:

- \*LOGGING (RECORDING=\*YES )

Der Protokollsatz muss aufgezeichnet werden, wenn die Bedingung zutrifft.

- \*LOGGING (RECORDING=\*NO )

Das Ereignis soll nicht aufgezeichnet werden, falls keine andere zutreffende Filterbedingung die Aufzeichnung verlangt.

Ein Protokollsatz wird also nur dann nicht aufgezeichnet, wenn alle auf ihn zutreffenden Filterbedingungen die Angabe TRIGGER-ACTION=\*LOGGING(RECORDING=\*NO) enthalten.

Trifft auf einen Protokollsatz keine Filterbedingung zu, wird er aufgezeichnet.

Der Filtermechanismus wird mit folgenden Kommandos gesteuert:

ADD-SAT-FILTER-CONDITIONS	Einrichten einer Filterbedingung
MODIFY-SAT-FILTER-CONDITIONS	Modifizieren einer Filterbedingung
REMOVE-SAT-FILTER-CONDITIONS	Entfernen einer Filterbedingung
SHOW-SAT-FILTER-CONDITIONS	Anzeigen einer Filterbedingung

Die Filterdefinitionen können in der SAT-Parameter-Datei gesichert werden, um sie bei der nächsten Sitzung wieder zu verwenden. Nicht explizit gesicherte Definitionen verfallen mit der Beendigung des Systemlaufs. Gesicherte Definitionen werden mit Beginn des nächsten Systemlaufs automatisch aktiviert.

### **Auswertung der Filterbedingungen**

Die Filterbedingungen werden nach der Preselection für die schaltbaren Benutzerkennungen und die nicht permanent sicherheitsrelevanten Ereignisse ausgewertet, die nicht bereits durch die Preselection entfernt wurden. Schaltbare Benutzerkennungen sind alle Benutzerkennungen, außer SYSAUDIT und den Kennungen mit dem Privileg SAT-FILE-MANAGEMENT oder SECURITY-Administration. Nicht permanent sicherheitsrelevante Ereignisse sind Ereignisse, deren Audit-Attribut veränderbar ist („J“ in der Spalte „Audit-Attribut Änd“ der [„Tabelle der Objekteignisse“ auf Seite 196ff](#)).

### **Hinweise zur Performance des Filtermechanismus**

Der Filtermechanismus bietet die Möglichkeit, durch den Vergleich mit der Information zu Ereignissen (Felder und ihre Inhalte) die Aufzeichnungsmenge gezielt zu verringern. Die dazu erforderlichen Vergleichsoperationen führen jedoch gegenüber der normalen Preselection zwangsläufig zu Performanceeinbußen in SATCP. Die Definition und der Einsatz von Filterbedingungen sollte daher sorgfältig überlegt werden.

### **Aktivierung eines Filters**

Ein Filter wird sofort nach seiner Definition (Kommando /ADD-SAT-FILTER-CONDITIONS) aktiv und bleibt es bis zum Ende des Systemlaufs oder bis er mit dem Kommando /REMOVE-SAT-FILTER-CONDITIONS gelöscht wird. Während dieser Zeit kann die Definition gespeichert, geändert oder angezeigt werden.

### 2.3.3 Verfeinern der Auswahl mit System-Exit Nr.110

Über den System-Exit Nr.110 kann die Systemverwaltung eine SAT-Exit-Routine zur Ausführung bringen. Die SAT-Exit-Routine ermöglicht es, die Aufzeichnung einiger protokollierbarer Ereignisse zu unterdrücken.

Die Beschreibung der generellen Arbeitsweise von System-Exits und eine detaillierte Beschreibung des System-Exit Nr.110 finden Sie im Handbuch „System Exits“ [18].

#### Ablaufschema für den System-Exit Nr. 110

Bevor der SATLOG-Satz in die SATLOG-Datei geschrieben wird, wird an den System-Exit eine Kopie des SATLOG-Satzes und die Information über dessen Länge übergeben. Anhand der Identifikatoren für die SAT-Information (siehe Tabellen ab [Seite 196](#)) kann der SATLOG-Satz analysiert werden.

Die SAT-Exit-Routine kann nun abhängig vom Analyseergebnis

- gezielte Reaktionen einleiten (z.B. Sperrung einer Benutzerkennung nach einer bestimmten Anzahl fehlerhafter LOGON-Versuche)
- einen eigenen SATLOG-Satz schreiben (Ereignis ANY, Makro \$SATANY)
- bei Rückkehr zu SAT über den Returncode das Schreiben des analysierten SATLOG-Satzes zulassen oder unterdrücken.

#### Sicherheitsvorkehrungen

Der Sicherheitsbeauftragte muss die Exit-Aufrufe mit dem Kommando `/MODIFY-SAT-PRESELECTION . . . ,EXIT=*YES` explizit erlauben.

An den Exit wird nur eine Kopie des Datensatzes übergeben. So ist sichergestellt, dass die Exit-Routine dessen Inhalt nicht verändern kann.

Die Exit-Routine wird nicht für Ereignisse aufgerufen, deren Protokollier-Einstellung nicht verändert werden kann. Sie wird auch nicht für das Ereignis ANY aufgerufen.

Exit-Routinen sind Subsysteme mit frei wählbaren Namen. Deshalb sollte in einem sicheren System die Systemverwaltung Namenskonventionen (insbesondere für den System-Exit Nr. 110) festlegen, die die Verbindung von Subsystemen zu Exit-Routinen eindeutig nachvollziehen lassen.

Der Sicherheitsbeauftragte hat keine Kontrolle über den Ablauf von Exit-Routinen. Deshalb sollte in einem sicheren System (insbesondere für den System-Exit Nr. 110) das Laden von Subsystemen generell überwacht werden. Der Sicherheitsbeauftragte muss dazu mittels `/MODIFY-SAT-PRESELECTION` die Ereignisse „Subsystem aktivieren“ (SCR), „Subsystem anhalten“ (SHD), „Subsystem fortsetzen“ (SRS) und „Subsystem deaktivieren“ (SDL) zur Protokollierung auswählen.

### 2.3.4 Nachbearbeitung von SATLOG-Dateien (Postselection)

Die Aufbereitung der SATLOG-Dateien ist Aufgabe der SAT-Datei-Verwaltung oder der SAT-Datei-Auswertung. Für die Aufbereitung steht das Dienstprogramm SATUT unter der Kennung SYSAUDIT zur Verfügung.

Es ist unabhängig vom SAT-Subsystem SATCP unter jeder Benutzerkennung ablauffähig, die das Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION besitzt.

SATUT kann neben SATLOG-Dateien auch CONSLOG-Dateien (siehe [Seite 221](#)) in die Auswertung einbeziehen.

Der SAT-Auswerter SATUT dient dazu,

- aus den Eingabedateien aufbereitete Dateien (replacement-files) zu erstellen, in denen die sicherheitsrelevanten Aufzeichnungen stehen, die die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung ausgewählt hat. In diesem Fall ist das Ziel die Reduktion der Datenmenge und Aufbewahrung der sicherheitsrelevanten SATLOG-Sätze, d.h. die Eingabedateien können durch die aufbereiteten Dateien ersetzt werden.
- aus den Eingabedateien mit Auswahlbedingungen bestimmte Protokolldatensätze auszuwählen. Diese werden auf Drucker (SYSLST) oder in eine XML-Datei ausgegeben, statistisch dargestellt oder in eine Datei (analysis-file) geschrieben. In diesem Fall ist das Ziel die Analyse ausgewählter Ereignisgruppen, d.h. die Eingabedateien werden nicht durch die aufbereiteten Dateien ersetzt.

Um Speicherplatz für SATLOG-Dateien einzusparen, sollten diese regelmäßig gewechselt (Kommando CHANGE-SAT-FILE), so bald wie möglich aufbereitet und durch replacement-files ersetzt oder auf Datenträger für langfristige Archivierung ausgelagert werden. Mit der Aufbereitung wird der Umfang der protokollierten Daten durch die feinere Auswahlmöglichkeit von SATUT reduziert.

Im folgenden Beispiel wird ein Batch-Job dargestellt, der unter der Benutzerkennung SYSAUDIT erstellt wurde und einmal pro Tag abläuft (Kommando ENTER-JOB mit REPEAT-JOB=\*DAILY). In diesem Job wird ein Job erstellt, der alle SATLOG-Dateien und replacement-files des Vortages ausgewertet, sofern ihr Name eine vierstellige Jahresangabe enthält. Das Ergebnis wird in einer einzigen analysis-file gespeichert. Danach werden die als Eingabe verwendeten SATLOG-Dateien automatisch gelöscht, replacement-files hingegen bleiben erhalten.

Um unbefugten Zugriff auf ausgedruckte Ausgabe-Protokolle zu verhindern, wird die Ausgabe, die auf die Systemdatei SYSLST erfolgt, in eine katalogisierte Datei umgelenkt. Diese kann z.B. mit SHOW-FILE auf dem Bildschirm untersucht werden.

```

/SET-LOGON-PARAMETERS
/REMARK *-----*
/REMARK * DIESER BATCH-JOB WERTET SATLOG-DATEIEN UND REPLACEMENT- *
/REMARK * FILES ANHAND DES DATUMS AUS. NUR DIE DATEIEN MIT DEM *
/REMARK * AELTESTEN DATUM WERDEN BEHANDELT. FUER DATEIEN DES *
/REMARK * AKTUELLEN TAGES FINDET KEINE AUSWERTUNG STATT. *
/REMARK * * *
/REMARK * SATLOG-DATEIEN WERDEN NACH IHRER AUSWERTUNG DURCH DIE *
/REMARK * PROZEDUR GELOESCHT, REPLACEMENT-FILES BLEIBEN ERHALTEN. *
/REMARK * * *
/REMARK * VORAUSSETZUNGEN: SAT-PROTOKOLLIERUNG MUSS AKTIV SEIN. DER *
/REMARK * NAME DER AKTUELLEN SATLOG-DATEI MUSS *
/REMARK * DAS DATUM MIT VIERSTELLIGER ANGABE DES *
/REMARK * JAHRES ENTHALTEN. *
/REMARK * EINGABEDATEIEN: SATLOG-DATEIEN UND/ODER REPLACEMENT- *
/REMARK * FILES, DEREN NAME DAS DATUM MIT VIER- *
/REMARK * STELLIGER ANGABE DES JAHRES ENTHAELT. *
/REMARK * AUSGABEDATEI: ANALYZE.<DATUM DER AUSGEWERTETEN DATEIEN> *
/REMARK *-----*
/ASSIGN-SYSOUT TO-FILE=BATCH.SYSOUT
/ASSIGN-SYSLST TO-FILE=BATCH.SYSLST
/ASSIGN-SYSDTA TO-FILE=*SYSCMD
/CHANGE-SAT-FILE
/SET-JOB-STEP
/MODIFY-JOB-SWITCHES ON=(4,5)
/START-EDT
@FSTAT 'SYS.SATLOG.////-*' TO 1
@PROC 1
  @@RENUMBER
  @@SET #L2=$
  @@IF #L2 = 1 GOTO 10
  @@NOTE NUR EINE DATEI GEFUNDEN -> KEINE DATEIEN VOM VORTAG
  @@SET #L3 = 1
  @@IF #L3:1-21 <> #L2:1-21 GOTO 20
  @@NOTE DATUM DER ERSTEN GEFUNDENEN DATEI GLEICH DATUM DER LETZTEN
  @@NOTE GEFUNDENEN DATEI -> ALLE DATEIEN VOM AKTUELLEN TAG
@10
  @@SET #S20 = 'KEINE ANALYSE DURCHGEFUEHRT. SIEHE WARNUNG '
  @@PRINT #S20 NSV
  @@RETURN
@20
  @@SET #L1 = 1
  @@ON #L1 FIND 'SYS.SATLOG.'
  @@NOTE DATUM EXTRAHIEREN
  @@SET #I2 = #I1 + 1
  @@SET #I3 = #I2 + 9
  @@SET #S1 = #L1:#I2-#I3
  @@DELETE

```

```

@@NOTE      SATUT-PROZEDUR ERSTELLEN
@@QUOTE !
@@CREATE 1  : !/SET-LOGON-PARAMETERS!
@@CREATE 2  : !/ASSIGN-SYSLST TO-FILE=LST.SEL.DAILY.!,#S1
@@CREATE 2.5 : !/ASSIGN-SYSOUT TO-FILE=OUT.SEL.DAILY.!,#S1
@@CREATE 3  : !/START-SATUT!
@@NOTE      DATEI DES VORHERGEHENDEN TAGES AUSWAEHLLEN
@@CREATE 4  : !//SELECT-INPUT-FILES INPUT-FILES=*STD(DATE=!,#S1,!))!
@@NOTE      DATEIEN NACH BESTIMMTEN VORGABEN AUSWAEHLLEN :
@@CREATE 5  : !//ADD-SELECTION-CONDITIONS NAME=PRIVI, CONDITION= -!
@@NOTE      BENUTZER AUSWAEHLLEN
@@CREATE 6  : !//      OBJ-UID  IN-LIST ('US1','US2','US3') -!
@@NOTE      INHALT DES ERGEBNISFELDES FESTLEGEN
@@CREATE 7  : !//AND  RES EQUAL F -!
@@NOTE      OBJEKT UEBER SEINE EREIGNISSE BESTIMMEN
@@CREATE 8  : !//AND  EVT IN-LIST ('PST','PRT') !
@@NOTE      SELEKTION DURCHFUEHREN
@@CREATE 8.5 : !//START-SELECTION FROM-FILE=*INPUT-FILES, - !
@@CREATE 8.7 : !//TO-FILE=*PAR(FILE=0, CONDITION-NAME=PRIVI) !
@@NOTE      AUSGEWAELHTE DATENSAETZE NACH SYSLST AUSGEBEN
@@CREATE 9  : !//SHOW-SELECTED-RECORDS SORT-CRITERION=*EVT, -!
@@CREATE 10 : !//      FROM-FILE=0, OUTPUT=*SYSLST(LINES=114) !
@@NOTE      AUSGEWAELHTE DATENSAETZE ZUR ARCHIVIERUNG IN EINE DATEI
@@NOTE      SCHREIBEN
@@CREATE 11 : !//SAVE-SELECTED-RECORDS TO-REDUCTION-NAME=ANALYZE.!,#S1
@@CREATE 12 : !//END!
@@CREATE 12.5 : !/SHOW-FILE-ATTRIBUTES ANALYZE.!,#S1
@@NOTE      BEARBEITETE SATLOG-DATEIEN LOESCHEN
@@CREATE 12.7 : !/DELETE-FILE SYS.SATLOG.!,#S1,!.,IGNORE=ACCESS!
@@CREATE 14  : !/SET-JOB-STEP!
@@CREATE 15  : !/ASSIGN-SYSLST TO-FILE=*PRIMARY!
@@CREATE 15.5 : !/ASSIGN-SYSOUT TO-FILE=*PRIMARY!
@@CREATE 16  : !/EXIT-JOB SYSTEM-OUTPUT=*NONE!
@@QUOTE '
@@WRITE 'E.RUN-DAILY' 0
@@SYSTEM 'ENTER-JOB E.RUN-DAILY', REPEAT-JOB = *DAILY
@END
@DO 1
@HALT
/MODIFY-JOB-SWITCHES OFF=(4,5)
/ASSIGN-SYSDTA TO-FILE=*PRIMARY
/ASSIGN-SYSLST TO-FILE=*PRIMARY
/EXIT-JOB SYSTEM-OUTPUT=*NONE

```

## 2.3.5 Überwachung spezieller sicherheitsrelevanter Aktivitäten

Bevor der Sicherheitsbeauftragte bestimmte sicherheitsrelevante Aktivitäten überwachen kann, muss er zunächst definieren, welche Ereignisse bei diesen Aktivitäten auftreten können. In diesem Abschnitt werden exemplarisch einige solcher Problemstellungen aufgezeigt. Die Angabe einer Preselection reduziert die anfallende Datenmenge der laufenden Session.

Beispiele für die Bildung komplexer Bedingungsausdrücke finden Sie auf [Seite 153](#). Ein ausführliches Auswertungsbeispiel mit SATUT finden Sie auf [Seite 188](#).

### Potenzielle Eindringversuche erkennen

Um potenzielle Eindringversuche bei LOGON zu erkennen, sollen alle fehlgeschlagenen Zugangsversuche ausgewertet werden. Dazu wählt der Sicherheitsbeauftragte das Ereignis „Userid prüfen“ (UCK) mit Ergebnis „FAILURE“ für die Protokollierung aus.

Auswahl bei Preselection:

```
/modify-sat-preselection -
/          event-auditing=uck(audit-switch=*on(result=*failure))
```

Zur Protokollierung fehlgeschlagener Zugangsversuche erfolgt die Einstellung für die Auswertung (Postselection) analog:

```
//add-selection-conditions name=conlog1, -
//          condition=evt equal 'uck' and res equal f
//start-selection from-file=*input-files, -
//          to-file=*par(condition-name=conlog1)
```

### Dateimanipulationen erkennen

Als Dateimanipulation kann man die erfolgreiche Durchführung folgender Ereignisse betrachten: „Datei erstellen“ (FCD), „Datei modifizieren“ (FMD), „Datei löschen“ (FDD), „Datei umbenennen“ (FRN), „Schutzattribute löschen“ (FDS), „Datei in entschlüsselte Datei umwandeln“ (FDC) und „Datei in verschlüsselte Datei umwandeln“ (FEC). Sie sollen daher mit dem RESULT=SUCCESS zur Protokollierung ausgewählt werden.

Auswahl bei Preselection:

```
//modify-sat-preselection -
//          event-auditing=(fcd(audit-switch=*on(result=*success)), -
//          ..., -
//          fec(audit-switch=*on(result=*success)))
```

Einstellung für die Auswertung (Postselection):

```
//add-selection-conditions name=confile, -
//    condition=evt in-list ('fcd','fmd','fdd','frn','fds','fdc','fec') -
//    and -
//    res equal s and filename equal '<destroyed file name>'
//start-selection from-file=*input-files, -
//    to-file=*par(condition-name=confile)
```

### Protokollierung von UTM-Ereignissen

Die Protokollierung von UTM-Ereignissen (TRM) kann sowohl in SAT, wie auch in openUTM gesteuert werden.

Auswahl bei Preselection:

```
/modify-sat-preselection event-auditing= -
/    trm(audit-switch=<*on/*off>(result=<*all/*success/*failure>), -
/    user-auditing=(<utm-userid1>,<utm-userid2>,...)
```

Einstellung für die Auswertung (Postselection):

```
//add-selection-conditions name=conutm, -
//    condition=evt equal 'trm' and <conditions>...
//start-selection from-file=*input-files, -
//    to-file=*par(condition-name=conutm)
```

Die Steuerung und Einstellung der SAT-Protokollierung für eine UTM-Anwendung erfolgt per UTM-Generierung und per UTM-Administration. Die UTM-SAT-Administration erfolgt durch dazu berechnigte UTM-Benutzer.

Soll die SAT-Protokollierung jedoch bereits mit dem Start einer UTM-Anwendung beginnen, so kann dies nur über die UTM-Generierung erreicht werden. Generierte Protokollierungswerte können durch KDCMSAT verändert werden.

Ausführliche Informationen zur SAT-Protokollierung finden Sie im openUTM-Handbuch „Anwendungen generieren“ [17].

### 2.3.6 SAT-Alarm

Die SAT-Alarm-Funktion erweitert den SAT-Funktionsumfang um eine wirksame Kontrollfunktion, mit der Verstöße gegen Sicherheitsmaßnahmen oder missbräuchliches Verhalten im laufenden Betrieb sofort aufgespürt werden können.

Mit der SAT-Alarm-Funktion erkennt der Sicherheitsbeauftragte missbräuchliches Verhalten sofort und nicht erst bei Auswertung der SATLOG-Dateien, da an der Konsole der Systembedienung eine Meldung ausgegeben wird, die den Verstoß anzeigt. Dies ist besonders von Vorteil, wenn Sicherheitsverstöße von Anwendern begangen werden. Der klassische Fall des Ausprobierens von Kennwörtern ist ein Beispiel für Sicherheitsverstöße von Anwendern.

Die SAT-Alarm-Funktion ersetzt nicht die SAT-Protokollierung und Auswertung der SATLOG-Dateien, da auch die von der Alarm-Funktion erkannten Verstöße in die SATLOG-Datei eingetragen werden. Auch schwächt eine Vielzahl von Alarmen zu unterschiedlichen Ereignissen den Aufmerksamkeitswert des Alarms deutlich ab. Es sollte daher gut überlegt werden, welche Ereignisse einen Alarm auslösen.

Ob ein SAT-Alarm in Form einer Meldung auf Konsole ausgelöst wird, hängt ab

- vom Ereignis und seinem Ergebnis
- von der Benutzerkennung
- von der Information in Verbindung mit dem Ereignis
- vom Zeitraum innerhalb dessen eine bestimmte Anzahl von Ereignissen eintrat

Die SAT-Alarm-Funktion wird gesteuert mit den folgenden Kommandos:

ADD-SAT-ALARM-CONDITIONS	formuliert eine neue Alarmdefinition
MODIFY-SAT-ALARM-CONDITIONS	ändert eine bestehende Alarmdefinition
REMOVE-SAT-ALARM-CONDITIONS	löscht eine bestehende Alarmdefinition
SHOW-SAT-ALARM-CONDITIONS	zeigt bestehende Alarmdefinitionen an

Die Alarmdefinitionen können in der SAT-Parameter-Datei gesichert werden, um sie bei der nächsten Sitzung wieder zu verwenden. Nicht explizit gesicherte Definitionen verfallen mit der Beendigung des Systemlaufs. Gesicherte Definitionen werden mit Beginn des nächsten Systemlaufs automatisch aktiviert.

### **Aktivierung einer Alarmdefinition**

Die Alarm-Funktion ist nur aktiv, wenn auch SAT im Aufzeichnungsmodus ist. Wurde SAT angehalten (/HOLD-SAT-LOGGING), wird auch kein Alarm gegeben. Bei angehaltenem SAT können keine neuen Alarmdefinitionen eingegeben oder bestehende verändert werden.

Ist SAT im Aufzeichnungsmodus, wird eine Alarmdefinition sofort nach ihrer Formulierung (/ADD-SAT-ALARM-CONDITIONS) aktiv und bleibt so bis zum Ende des Systemlaufs oder bis sie mit /REMOVE-SAT-ALARM-CONDITIONS gelöscht wird. Während dieser Zeit kann die Definition gespeichert, geändert oder angezeigt werden.

Hat der Sicherheitsbeauftragte für ein Produkt den Anschluss an das SAT-Logging mit /MODIFY-SAT-SUPPORT-PARAMETERS deaktiviert, so ist die Alarm-Funktion für die zu diesem Produkt gehörenden Ereignisse nicht aktiv. (In der aktuellen SECOS-Version gilt dies für die Ereignisse der Objekte „POSIX-FILE-and-Directory“, „POSIX-CHILD-Process“, „POSIX-PROCESS“, „POSIX-SYSTEM-Resources“).

### **Wirkungsweise der Alarmfunktion**

Die Alarmfunktion wird unabhängig von der Preselection für jedes protokollierbare Ereignis aufgerufen. Dann werden alle definierten Alarmbedingungen geprüft, ob sie auf den aktuellen Protokolldatensatz zutreffen. Eine Alarmbedingung trifft dann auf einen Protokolldatensatz zu, wenn alle in ihr enthaltenen Teilbedingungen wahr sind. Eine Bedingung, in der ein Feldname enthalten ist, ist nur dann wahr, wenn dieses Feld im Protokolldatensatz enthalten ist. Falls eine Negativliste angegeben ist, ist die Bedingung wahr, wenn keines der darin angegebenen Felder im Protokolldatensatz enthalten ist. Falls eine Alarmdefinition in allen Teilbedingungen auf einen Protokolldatensatz zutrifft, wird eine Warnung auf Konsole ausgegeben.

## 2.4 Verwalten von SAT

### 2.4.1 SAT-Subsystem SATCP

SATCP (SAT Control Program) ist der Teil von SAT zur Überwachung von Ereignissen und Alarmen. Das Subsystem SATCP wird beim STARTUP von DSSM automatisch erstellt und gestartet. SATCP ist somit vor SYSTEM READY bereit. Standardmäßig ist SATCP aktiv und protokolliert in die erste neue SATLOG-Datei des Systemlaufs. Ihr Name entspricht dem Standardnamen mit der Folgenummer 1.

Zusätzlich kann der Sicherheitsbeauftragte mit den Kommandos /HOLD-SAT-LOGGING und /RESUME-SAT-LOGGING die Protokollierung mit SAT anhalten und anschließend wieder starten.

Wenn durch einen DVS-Fehler das Öffnen der ersten SATLOG-Datei nicht möglich ist, wird SATCP zwar geladen, aber in den HOLD-Zustand versetzt. Es wird eine Warnung an die Konsole gesendet. Die Protokollierung muss dann mit dem Kommando /RESUME-SAT-LOGGING wieder aufgenommen werden.

Wurde ein vorheriger Systemlauf abnormal beendet, überprüft SATCP, ob die SATLOG-Dateien korrekt geschlossen wurden und verifiziert sie bei Bedarf.

Der Sicherheitsbeauftragte darf SATCP mit dem Kommando /HOLD-SAT-LOGGING anhalten, d.h. die Protokollierung aller Ereignisse wird ausgesetzt, und die aktuelle SATLOG-Datei wird geschlossen. SAT protokolliert dann keine Ereignisse, nimmt aber bei einem nachfolgenden Kommando /RESUME-SAT-LOGGING die Protokollierung mit genau den Parametern wieder auf, die vor dem Kommando /HOLD-SAT-LOGGING Gültigkeit hatten.

Das SATCP-Subsystem wird beim SHUTDOWN automatisch deaktiviert. Es kann nicht mit dem Kommando /STOP-SUBSYSTEM oder dem entsprechenden Makro deaktiviert werden.

## 2.4.2 SAT-Parameter-Datei

Die SAT-Parameter-Datei enthält alle Angaben, um SAT bei einer folgenden Sitzung mit eigenen Einstellungen starten zu lassen. Einstellungen können von Kennungen mit dem Privileg SAT-FILE-MANAGEMENT oder SECURITY-ADMINISTRATION vorgenommen werden.

SAT-Parameter werden nicht automatisch in der SAT-Parameter-Datei gespeichert, sondern müssen explizit gespeichert werden. Dies geschieht mit dem Kommando SAVE-SAT-PARAMETERS (siehe [Seite 120](#)). Beim Speichern kann bestimmt werden, welche Werte (\*STANDARD oder \*CURRENT) in die Parameterdatei übernommen werden sollen.

Abhängig vom Privileg des Kommandoaufrufers werden folgende Parameter in der SAT-Parameter-Datei gespeichert:

- EVENT-PRESELECTION (mit Privileg SECURITY-ADMINISTRATION)
- ALARM-CONDITIONS (mit Privileg SECURITY-ADMINISTRATION)
- FILTER-CONDITIONS (mit Privileg SECURITY-ADMINISTRATION)
- SAT-FILE-ATTRIBUTES (mit Privileg SAT-FILE-MANAGEMENT)
- SAT-SUPPORT (mit Privileg SECURITY-ADMINISTRATION)

Die SAT-Parameter-Datei \$SYSAUDIT.SYSPAR.SAT wird auf dem Home-Pubset als ISAM-Datei angelegt mit den Attributen ACCESS=READ, BLKSIZE=(STD,2), DESTROY=YES und AUDIT=ALL.

Die SAT-Parameter-Datei wird bei der Initialisierung des SATCP-Subsystems (beim STARTUP) geöffnet, die in ihr enthaltenen Parameter werden übernommen. Existiert zu diesem Zeitpunkt keine SAT-Parameter-Datei, so wird sie erstellt, und SAT startet mit den Standard-Werten.

Die SAT-Parameter-Datei bleibt geöffnet, während das SATCP-Subsystem aktiv ist. Alle Zugriffe auf die SAT-Parameter-Datei finden unter der Kontrolle einer System-Task statt (SATP-Task). So wird sichergestellt, dass auf die SAT-Parameter-Datei nicht unerlaubt zugegriffen werden kann.

Treten beim Öffnen Fehler auf, so verfährt SAT wie folgt: Trat der Fehler im DVS oder der SATP-Task-Umgebung (SAT-Subsystem) auf, versucht SAT, die SAT-Parameter-Datei wiederherzustellen und sie erneut zu öffnen. Gelingt dies nicht, wird die aktuelle Datei geschlossen (falls möglich) und die SATP-Task-Umgebung freigegeben. Dieser Vorgang wird an der Konsole gemeldet. Der SAT-Datei-Verwalter kann dann auf die SAT-Parameter-Datei zugreifen, um die Fehlerursache zu ermitteln und geeignete Maßnahmen zu ergreifen.

Ein Fehler in der SAT-Parameterdatei hat keine Auswirkungen auf die SAT-Protokollierung oder SAT-Alarm-Funktion. Allerdings werden dann statt der in der Parameterdatei gespeicherten Werte die Standard-Vorgaben verwendet.

Der Fehler könnte durch folgende Maßnahmen behoben werden:

- Der SAT-Datei-Verwalter katalogisiert die fehlerhafte SAT-Parameterdatei unter einem neuen Namen, um sie zu Diagnosezwecken zur Verfügung zu stellen. Falls dies nicht möglich ist, löscht er sie.
- Anschließend fährt er das System neu hoch. Wenn währenddessen keine SAT-Parameterdatei vorhanden ist, legt SATCP diese mit Standardwerten neu an.
- Schließlich stellt der SAT-Datei-Verwalter die aktuellen SAT-Parameterwerte neu ein und speichert sie mit dem Kommando /SAVE-SAT-PARAMETERS und der Angabe \*CURRENT für die gewünschten Operanden.

### **Erstmalige Installation von SAT**

Beim ersten Systemstart nach erstmaliger Installation von SAT existiert noch keine SAT-Parameter-Datei. In diesem Fall startet das SATCP-Subsystem mit den Standard-Werten und legt automatisch eine SAT-Parameter-Datei mit diesen Werten an. In allen folgenden Sitzungen startet SATCP mit den Werten, die dann in dieser Datei abgespeichert sind.

### **Umstieg auf eine neue Version**

Die SAT-Parameter-Datei enthält SAT-Parameter für den nächsten Systemlauf. Ist zwischen zwei Sitzungen ein Versionswechsel auf eine höhere Version erfolgt, erkennt die Folgeversion das ältere Format und adaptiert die ältere Datei wie folgt:

- Alte Parameter werden kopiert und bleiben erhalten. Die Kopien werden im Format an die neue Version adaptiert.
- Neu hinzugekommene Parameter werden mit ihren Standard-Werten ergänzt.

#### *Hinweis*

Sind in der alten SAT-Parameter-Datei statt konkreter Werte auch Typen für Operandenwerte gespeichert (z.B. \*STANDARD, \*CURRENT), werden diese unverändert übernommen. Es wird von SAT nicht überprüft, ob diese Typen in der neuen Version eine andere Semantik bekommen haben.

## Beispiele zur SAT-Parameter-Datei

### *Änderung der SAT-Parameter-Datei*

In der aktuellen Sitzung wurden Werte für die Ereignis-Auswahl mit dem Kommando /MODIFY-SAT-PRESELECTION und die Dateiattribute der SATLOG-Datei mit dem Kommando /CHANGE-SAT-FILE verändert. Alarm- und Filterbedingungen sowie die Einstellung der SAT-Support-Parameter wurden in dieser Sitzung nicht verändert.

Der **Sicherheitsbeauftragte** speichert die aktuell gültigen Werte mit folgendem Kommando in der SAT-Parameter-Datei ab:

```

/save-sat-parameters event-preselection=*current, -
/                      alarm-conditions=*current, -
/                      filter-conditions=*current, -
/                      sat-support=*current

```

Die nächste Sitzung würde mit folgenden Einstellungen beginnen:

EVENT-PRESELECTION	Werte, die bei der Eingabe des Kommandos SAVE-SAT-PARAMETERS gültig waren
ALARM-CONDITIONS	Werte wie in der letzten Sitzung, da sie bei der Ausführung des Kommandos SAVE-SAT-PARAMETERS nicht verändert waren
FILTER-CONDITIONS	Werte wie in der letzten Sitzung, da sie bei der Ausführung des Kommandos SAVE-SAT-PARAMETERS nicht verändert waren
SAT-FILE-ATTRIBUTES	Werte wie in der letzten Sitzung, da sie nicht gespeichert wurden
SAT-SUPPORT	Werte wie in der letzten Sitzung, da sie bei der Ausführung des Kommandos SAVE-SAT-PARAMETERS nicht verändert waren

Der **SAT-Datei-Verwalter** möchte die Veränderungen an den Attributen der SATLOG-Datei ebenfalls in die SAT-Parameter-Datei übernehmen. Dazu verwendet er folgendes Kommando:

```
/save-sat-parameters sat-file-attributes=*current
```

Deshalb beginnt die nächste Sitzung mit folgenden Einstellungen:

EVENT-PRESELECTION	Wie oben
ALARM-CONDITIONS	Wie oben
FILTER-CONDITIONS	Wie oben
SAT-SUPPORT	Wie oben
SAT-FILE-ATTRIBUTES	Werte, die bei der Eingabe des Kommandos SAVE-SAT-PARAMETERS gültig waren

### 2.4.3 SAT-Protokolldateien (SATLOG)

Eine SATLOG-Datei besteht aus SATLOG-Sätzen, die sicherheitsrelevante Ereignisse beschreiben.

Die SATLOG-Dateien werden auf den Standard-Pubset der Benutzerkennung SYSAUDIT mit folgendem Namen angelegt:

`$_SYSAUDIT.SYS.SATLOG.yyyy-mm-dd.sss.nn` wobei:

yyyy-mm-dd	Erstellungsdatum
sss	session-number
nn	Nummer der Datei in diesem Systemlauf (01 bis 99).

Die SATLOG-Dateien werden als SAM-Dateien mit dem Attribut DESTROY=YES im EXTEND-Modus mit Blockgröße (STD,2), Speicherplatzzuweisung (120,120) und AUDIT-ATTRIBUT = ALL angelegt.

Aus Performancegründen wird das Schreiben der SAT-Sätze in die SATLOG-Datei von einer getrennten Task ausgeführt. SAT bedient sich dabei der CLTF-Schnittstelle (Common Log Task Facility).

#### 2.4.3.1 Schutz der SATLOG-Dateien

Nur Benutzer mit dem Privileg SAT-FILE-EVALUATION oder SAT-FILE-MANAGEMENT können SATLOG-Dateien auswerten. Die Dateien müssen so geschützt werden, dass sie nur von den Kennungen zugreifbar sind, die mit dem Privileg SAT-FILE-EVALUATION oder SAT-FILE-MANAGEMENT ausgestattet sind. Optimalen Schutz erreicht man, wenn SATLOG-Dateien und reduzierte SAT-Protokolldateien mit einem Guard verknüpft sind. Dieses Guard kann dann die Bedingungen enthalten, dass nur mit einem bestimmten Privileg und nur mit einem bestimmten Programm auf die SAT-Dateien zugegriffen werden darf.

Zusätzlich werden alle Zugriffe auf die SAT-Dateien automatisch protokolliert (bei Verknüpfungsregel INDEPENDENT), weil das Audit-Attribut gesetzt ist. Dies gilt auch für das Öffnen, Schließen und Wechseln der SATLOG-Dateien.

Folgende Hinweise sind – besonders bei der Vergabe des Privilegs SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION an andere Benutzerkennungen als SYSAUDIT – zu beachten:

- Die Auswertung der SATLOG-Dateien, die unter SYSAUDIT katalogisiert sind, ist nur möglich, wenn diese mehrbenutzbar sind. Mit der SRPM-Gruppenverwaltung sollte eine AUDITOR-Gruppe eingerichtet werden, die die Benutzerkennung SYSAUDIT enthält. Mit der einfachen Zugriffskontrollliste (BACL) oder einem Guard sollten die Dateien für die AUDITOR-Gruppe zugreifbar gemacht werden.

- Das Löschen von SATLOG-Dateien und das Erstellen von replacement-files mit SATUT ist nur unter der Benutzerkennung SYSAUDIT möglich. Analysis-files oder Listen können auch unter einer anderen Benutzerkennung erzeugt werden (siehe [Abschnitt „Eingabedateien für SATUT“ auf Seite 141ff](#)).

### 2.4.3.2 Wechseln der SATLOG-Dateien

Mit dem Kommando CHANGE-SAT-FILE können der Sicherheitsbeauftragte und der SAT-Datei-Verwalter SATLOG-Dateien wechseln.

Der SAT-Datei-Verwalter kann dabei die SATLOG-Dateien auch auf private Platten und Bänder legen und die Dateiattribute verändern.

Bei geschlossenen SATLOG-Dateien kann der Katalogeintrag mit ACCESS=READ und SPACE = RELEASE(-9999) optimiert werden.

#### Explizites Wechseln

Wenn die aktuelle SATLOG-Datei zu groß wird oder wenn sie gewechselt werden muss, kann sie per Kommando gewechselt werden. Die SAT-Datei-Verwaltung kann die aktuelle SATLOG-Datei mit dem Kommando CHANGE-SAT-FILE schließen und eine neue SATLOG-Datei eröffnen, ohne dass Daten verlorengehen.

#### Implizites Wechseln

Wenn in der aktuellen SATLOG-Datei ein DVS-Fehler auftritt (einschließlich Speichersättigung), wird die SATLOG-Datei implizit gewechselt, d.h. ohne Einfluss der SAT-Datei-Verwaltung. Dabei kann es vorkommen, dass bei einigen DVS-Fehlern der Trailer-Satz nicht geschrieben werden kann (z.B. bei „no disc space available“, d.h. wenn die primäre Speicherplatzzuweisung ausgeschöpft ist und die sekundäre Speicherplatzzuweisung Null ist).

#### Periodisches Wechseln

Mit dem Operanden REPEAT des Kommandos /CHANGE-SAT-FILE kann die aktuelle SATLOG-Datei in festen Zeitabständen automatisch gewechselt werden. Dabei gehen keine Daten verloren.

Eine Zeitperiode beginnt mit der Eingabe des Kommandos /CHANGE-SAT-FILE oder durch das Kommando /RESUME-SAT-LOGGING, falls die Protokollierung mit SAT angehalten war.

### 2.4.3.3 Speicherplatzbedarf

Der Speicherplatzbedarf für die SAT-Protokollierung wächst mit der Anzahl der Ereignisse, die protokolliert werden. Man kann die Anzahl der zu protokollierenden Ereignisse reduzieren, wenn für die Protokollierung der Ereignisse zusätzliche Kriterien festgelegt werden, die deren Protokollierung einschränken (siehe [Abschnitt „Auswahlverfahren“ auf Seite 21](#)). Damit hat der Sicherheitsbeauftragte mit der Festlegung der Auswahl-Kriterien großen Einfluss auf den Speicherplatzbedarf von SAT.

Die tatsächlich protokollierte Datenmenge ist abhängig von Größe und Auslastung der Anlage und vom Anwendungsspektrum. Es ist empfehlenswert, den entsprechenden Speicherplatzbedarf in Probeläufen oder mit Hilfe der SATUT-Anweisung //SHOW-STATISTICS (siehe [Seite 174ff](#)) zu ermitteln.

Folgendes Rechenbeispiel soll eine Vorstellung vermitteln:

Bei der Standard-Protokollier-Einstellung (es wurde kein Kommando /MODIFY-SAT-PRESELECTION abgesetzt) und Audit-Attribute NONE für alle FILE-Objekte wurden folgende Durchschnittswerte ermittelt:

- Länge eines Protokoll-Datensatzes: 75-80 Byte
- Anzahl protokollierter Ereignisse: 700-800 Ereignisse/MIP/Std
- Benötigter Plattenspeicherplatz: 30-35 PAM-Seiten/MIP/Std

Besonders die Audit-Attribute der FILE-Objekte (siehe [Abschnitt „Auswahlverfahren“ auf Seite 23](#)) können den Speicherplatzbedarf von SAT beeinflussen, denn Ereignisse, die FILE-Objekte betreffen, machen ca. 50% aller möglichen Ereignisse aus. Sie werden entsprechend ihres Ergebnisses und ihres Audit-Attributs protokolliert.

## Speichersättigung

Wenn Speicherplatzprobleme auftreten (auf den gemeinschaftlich nutzbaren Plattenspeichern ist kein weiterer Speicherplatz verfügbar), verhindert ein DVS-Fehler die weitere Protokollierung mit SAT. Um einen Verlust von Protokollinformation zu vermeiden, stellt SAT die Aufträge, die einen SATLOG-Satz schreiben wollen, zurück (Makro VPASS siehe Handbuch „Makroaufrufe an den Ablaufteil“ [15]). Die Aufträge der Kennungen mit dem Privileg SECURITY-ADMINISTRATION und SAT-FILE-MANAGEMENT werden weiter protokolliert, da deren SATLOG-Sätze so lange im Klasse-5-Speicher abgelegt werden, bis die Situation sich wieder normalisiert hat. Bei einem /EXIT-JOB bzw /LOGOFF gehen die SATLOG-Sätze der letztgenannten Kennungen nicht verloren und das Kommando wird wie folgt ausgeführt:

- die Verbindung zum Terminal wird geschlossen
- die Task wird solange nicht beendet, bis SATCP wieder in den Protokollierstatus wechselt
- ein /SET-LOGON-PARAMETERS bzw. /LOGON für nichtprivilegierte Benutzer wird abgewiesen, das sind alle Benutzer außer denen mit den Privilegien SECURITY-ADMINISTRATION, SAT-FILE-MANAGEMENT oder OPERATING.

Wenn der SAT-Status auf NO-RESOURCE schaltet, wird eine Meldung über die Art des Problems an der Konsole ausgegeben. Der Sicherheitsbeauftragte und die SAT-Datei-Verwaltung können Maßnahmen ergreifen und SAT setzt die Protokollierung automatisch fort.

### *Beispiel*

Bei „disc space saturation“:

```
/change-sat-file ... ,support=*private-volume(...)
```

Aufträge, deren SATLOG-Sätze im Klasse-5-Speicher abgelegt wurden, während sich SATCP im Status NO-RESOURCE befand, bleiben unter Umständen auch nach der Eingabe des Kommandos /HOLD-SAT-LOGGING zurückgestellt (Makro VPASS, siehe Handbuch „Makroaufrufe“ [15]). In diesem Fall gibt SATCP in regelmäßigen Abständen eine Meldung aus, die auf diesen Zustand hinweist. Um die Verarbeitung der zurückgestellten Aufträge fortzusetzen, ist zusätzlich die Eingabe des Kommandos /RESUME-SAT-LOGGING erforderlich.

#### 2.4.3.4 Aufbau der SATLOG-Dateien

Alle SATLOG-Sätze haben dieselbe Struktur. Sie bestehen aus einer Liste von Feldern, wobei jedes dieser Felder eine protokollierbare Information enthält.

Werden ausschließlich SAT-Kommandos und SATUT-Anweisungen verwendet, so ist keine Kenntnis über den Aufbau der SATLOG-Dateien erforderlich.

Nur bei Anwendung des System-Exit Nr. 110 oder bei einer expliziten Dateianalyse im Fehlerfall sind die nachfolgenden Informationen von Bedeutung.

##### *Hinweis*

Die Struktur der Datensätze ist versionsabhängig und wird durch den Makro EXIT110 beschrieben (siehe Handbuch „System-Exits“ [18]).

#### **Header-/Trailer-Sätze**

Den SATLOG-Sätzen sind SAT-eigene SATLOG-Sätze voran- bzw. nachgestellt, die sich auf die besonderen Ereignisse „Beginn/Ende der SATLOG-Datei“ beziehen.

Der Header-Satz (ZBG) beinhaltet:

- die Systemversion
- den Systemnamen
- Grund für das Erstellen der Datei (STARTUP, resume logging...)
- Name der vorhergehenden SATLOG-Datei (falls vorhanden)
- Kennzeichnung der CPU
- Kennzeichnung des Systems
- Name der Konfiguration

Der Trailer-Satz (ZND) beinhaltet:

- den Namen der folgenden SATLOG-Datei dieses Systemlaufs
- Grund für das Schließen der Datei (SHUTDOWN, change file...)

**Datensätze**

Die Felder jedes SATLOG-Satzes sind folgendermaßen angeordnet:

- Der erste Satzteil ist ein fester Teil, in dem die Felder enthalten sind, die für jeden Datensatz protokolliert werden.

Feldname	Länge	Bedeutung	
user-id	8	Benutzerkennung des Subjekts	fester Teil Länge 28 Zeichen
tsn	4	TSN des Subjekts	
evt	3	Kurzname für Ereignis	
res	1	Resultat des Ereignisses (S/F)	
	4	Erstellungsdatum Format: X'yyyymmdd'	
	4	Erstellungszeit Format: X'hmmss00'	
	4	reservierter Bereich	

- Der folgende Satzteil ist variabel.  
Er enthält zum einen die Felder, die bei jedem Datensatz protokolliert werden können, aber optional sind (z.B. auditid, groupid). Zum andern enthält er die Felder, die für ein bestimmtes Objekt protokolliert werden (siehe [Abschnitt „Tabellen der protokollierbaren Information je Objekt ereignis“ auf Seite 213ff](#)). Diese Felder haben variable Länge. Jedes Feld des variablen Teils beinhaltet die reale Länge der Information, den Exit-Identifikator für die SAT-Information und die Information selbst.

In1	id1	<info1>	variabler Teil variable Länge
In2	id2	<info2>	
In3	id3	<info3>	
...	...	...	

- In n: Länge der protokollierten Information <info n> des Feldes n (1 Byte).  
Bei \*LNG-Feldern enthält dieses Feld den Wert 255.
- id n: Exit-Identifikator für die SAT-Information, die in Feld n steht (2 Byte).  
Bei \*LNG-Feldern enthält dieses Feld den negativen Wert des Exit-Identifikators.
- info n: protokollierte Information des Feldes n (Feldwert, In n Byte),  
Keywords sind dabei binär codiert

*\*LNG-Felder*

\*LNG-Felder sind Felder, deren Länge größer ist als 255 Zeichen. Sie werden nötigenfalls auf mehrere Protokollsätze aufgeteilt und sind folgendermaßen aufgebaut:

255	- id	In	0	<info1>	Erster oder einziger Protokollsatz für das *LNG-Feld
255	- id	In	distanz	<info n>	Folgesatz für ein *LNG-Feld, wenn dieses über mehrere Protokollsätze aufgeteilt ist

- In: Gesamtlänge der protokollierten Information des \*LNG-Feldes (2 Byte).
- id: Exit-Identifikator für die SAT-Information, die in einem \*LNG-Feld steht (2 Byte, Wert ist negativ).
- distanz: Distanz des 1. Bytes des Teilbereichs „info n“ zum Anfang der gesamten Information
- info n: n-ter Teil der protokollierten Information des \*LNG-Feldes

Die Maximallänge eines SATLOG-Satzes in der SATLOG-Datei beträgt 1000. Der EXIT-Routine wird der ungeteilte SATLOG-Satz zur Verfügung gestellt. Die maximale Länge beträgt 32752 Bytes, *distanz* ist immer 0.

*Beispiel (Datensätze abdruckbar und sedezimal)*

-----1-----2-----3-----4-----5-----6-----7-----8 ...  
 <----- fester Teil -----><----- variabler Teil ...

TSOS 0AL6FEDS..... .q. ... .\*UNI. .:4V06:\$TSOS.PLAMLIB. ... ..  
 EEDE4444FCDFCCCE2102141900000005EDC1007FEFF75EEDE4DDCDDCC00000001  
 3262000001366542083330386033402C459303A4506AB3262B731439210581061

SYSAUDITOAMCFRSS.....f. ... .\*UNI. .:4V06:\$TSOS.EDT. ... .4V06. ..  
 EEECECCEFCDCDEE2102143800000005EDC0007FEFF75EEDE4CCE0000002FEFF0060  
 2821449301436922083342366033402C459F03A4506AB3262B543105840245061042

SYSAUDITOAMCXLDS.....g. ... .\*UNI. .:4V06:\$TSOS.EDT. .C. .EDT. .16.6A. .96-06-04 ...  
 EEECECCEFCDCEDCE2102143800000005EDC0007FEFF75EEDE4CCE000C000CCE000FF4FC000FF6FF6FF ...  
 2821449301437342083342376021402C459F03A4506AB3262B54310A330B54350C16B6180D96006004 ...

*Beispiel (obige Datensätze als SATUT-Ausgabe)*

EVT	RES	DATE	TIME	TSN	USER-ID			
FED	S	20180323	134013	0AL6	TSOS	GROUPID= *UNI	FILNAME= :4V06:\$TSOS.PLAMLIB	AUDITAT= NONE
						ACCESS = INPUT-EXECUTE		
FRS	S	20180323	144233	OAMC	SYSAUDIT	GROUPID= *UNI	FILNAME= :4V06:\$TSOS.EDT	AUDITAT= NONE
						CATID = 4V06	PSWDPAR= NO	
XLD	S	20180323	144233	OAMC	SYSAUDIT	GROUPID= *UNI	FILNAME= :4V06:\$TSOS.EDT	ELTTYPE= C
						INTNAME= EDT	INTVERS= 16.6A	INTDATE= 96-06-04
						LOADUNI= %ROOT	CXTNAME= CTXPHASE	MEMCLAS= CLASS6

## 2.4.4 Überwachung durch SAT-spezifische Jobvariable

Der Zustand der SAT-Protokollierung und der Name der aktuellen SATLOG-Datei können mit einer Jobvariablen überwacht werden. Diese Jobvariable hat den festen Namen `:<home-catid>:$SYSAUDIT.SYS.SAT.SATLOG-FILENAME`. Sie wird bei jedem Wechsel der SATLOG-Datei und bei jedem Wechsel des SAT-Zustands von SAT versorgt. Falls sie nicht existiert, wird sie automatisch unter der Kennung SYSAUDIT auf dem Home-Pubset angelegt.



Vom Beginn eines Systemlaufs bis zum ersten Wechsel der SATLOG-Datei ist der Inhalt der Jobvariable undefiniert.

Die Struktur der Jobvariable entspricht der für auftragsüberwachende Jobvariablen (siehe Handbuch „Jobvariablen“ [31]). Folgende Einträge haben SAT-spezifische Bedeutungen:

Byte	Bedeutung/mögliche Werte
1-3	SAT-Zustand: \$R: RECORD (Aufzeichnungsmodus) \$H: HOLD (d.h. es wurde das Kommando /HOLD-SAT-LOGGING ausgeführt) \$N: NO RESOURCE \$S: SHUTDOWN
17	Typ der MONJV: „A“
71-128	Name der SATLOG-Datei Im Aufzeichnungsmodus (SAT-Zustand = „\$R“) handelt es sich hierbei um die aktuelle SATLOG-Datei, in allen anderen Fällen um die gerade geschlossene SATLOG-Datei.

## 2.4.5 SAT - Installation und Inbetriebnahme

Die Installation von SAT umfasst die Installation der Software für das Subsystem SATCP und für das Dienstprogramm SATUT. Vor der Inbetriebnahme von SAT sollten Sie ein Konzept zur Protokollierung sicherheitsrelevanter Daten anhand der Steuerungsmöglichkeiten für SAT entwerfen. Siehe dazu [Abschnitt „Subjekt, Objekt und Ereignis“ auf Seite 16](#), [Abschnitt „Nachbearbeitung von SATLOG-Dateien \(Postselection\)“ auf Seite 33](#) und [Abschnitt „Überwachung spezieller sicherheitsrelevanter Aktivitäten“ auf Seite 36](#).

### SATCP installieren

Folgende Dateien müssen für SAT unter TSOS katalogisiert sein:

Datei	Name der Datei
Subsystemkatalog	\$TSOS.SYSSCC.SATCP.nnn
Subsystembibliothek – für SU_/390 und S-Server – für SU x86 und SQ-Server –	\$TSOS.SYSLNK.SATCP.nnn \$TSOS.SKMLNK.SATCP.nnn
Syntaxdatei	\$TSOS.SYSSDF.SATCP.nnn
Meldungsdatei	\$TSOS.SYSMES.SATCP.nnn
Korrekturdatei	\$TSOS.SYSRMS.SATCP.nnn
IMON-Datei	\$TSOS.SYSSII.SATCP.nnn
ENTER-Job für die Übernahme der Preselection bei Einsatz einer neuen SAT-Version	\$TSOS.SYSENT.SATCP.nnn

Tabelle 2: Installationsdateien für SATCP (nnn = Version des Subsystems)

Das Subsystem SATCP wird beim STARTUP automatisch von DSSM aktiviert und gestartet. SAT ist somit vor SYSTEM READY bereit. Standardmäßig ist SAT aktiv und protokolliert in die erste neue SATLOG-Datei des Systemlaufs. Beim SHUTDOWN wird das Subsystem SATCP implizit deaktiviert. Es kann nicht explizit deaktiviert werden.

In einem BS2000-System, in dem SECOS erstmalig zum Einsatz kommt, haben nach der Installation alle Benutzerkennungen die Protokollier-Einstellung AUDIT-SWITCH=\*ON.

In einem BS2000-System, das von einer niedrigeren SECOS-Version auf eine höhere SECOS-Version konvertiert wurde, behalten nach der Installation alle Benutzerkennungen die bisherige Protokollier-Einstellung.

Zur Sicherung der aktuellen Preselection-Einstellung der Benutzerkennungen vor einer Änderung wird ein ENTER-Job zur Verfügung gestellt. Diese generiert eine ENTER-Datei mit den entsprechenden /MODIFY-SAT-PRESELECTION-Kommandos.

## SATUT installieren

Folgende Dateien werden mit SATUT ausgeliefert:

<b>Datei</b>	<b>Name der Datei</b>
Modulbibliothek	<b>\$SYSAUDIT.SYSLNK.SATUT.nnn</b>
System-Syntaxdatei	<b>\$TSOS.SYSSDF.SATUT.nnn</b>
Meldungsdatei	<b>\$TSOS.SYSMES.SATUT.nnn</b>
Korrekturdatei	<b>\$TSOS.SYSRMS.SATUT.nnn</b>
IMON-Datei	<b>\$TSOS.SYSSII.SATUT.nnn</b>

Tabelle 3: Installationsdateien für SATUT (nnn = Version des Subsystems)

SATUT läuft unabhängig von SAT unter jeder Benutzerkennung mit dem Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION.

## 2.5 SAT-Kommandos

In diesem Abschnitt werden alle SAT-Kommandos in alphabetischer Reihenfolge aufgeführt. Die Beschreibung der Kommandos ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion des Kommandos erklärt, dann folgt das Kommandoformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung folgt der Kommando-Returncode und gegebenenfalls ein Anwendungsbeispiel.

Die Metasyntax zu den Kommandos finden Sie im Anhang des Handbuchs.

### Funktionelle Übersicht

#### Produktspezifische Aktivierung und Deaktivierung von Protokollierung und Alarmen

MODIFY-SAT-SUPPORT-PARAMETERS	Aktivierung oder Deaktivierung der SAT-Protokollierung und der SAT-Alarme für ein bestimmtes Produkt
SHOW-SAT-SUPPORT-PARAMETERS	Anzeige, für welches Produkt die SAT-Protokollierung sowie die Auslösung der SAT-Alarme generell aktiviert oder deaktiviert ist

#### SAT-Vorabauswahl (Preselection)

MODIFY-SAT-PRESELECTION	Änderung der Auswahl von Ereignissen (EVENT-AUDITING) und Benutzerkennungen (USER-AUDITING), Änderung der Verknüpfungsregel (PRESELECTION-RULE), Änderung der Erlaubnis für den Aufruf des System-Exits Nr. 110 (EXIT) und Festlegung des Aufzeichnungsumfangs
SAVE-SAT-PARAMETERS	Speicherung der spezifizierten SAT-Parameter für den nächsten Systemstart in einer SAT-Parameter-Datei
SHOW-SAT-STATUS	Anzeige der ausgewählten Benutzerkennungen, Ereignisse und der eingestellten Verknüpfungsregel (... INFORMATION=*USER-AUDITING /*EVENT-AUDITING/*PRESELECTION-RULE)

**SAT-Filtermechanismus**

ADD-SAT-FILTER-CONDITIONS	Definition von Bedingungen zur Vorauswahl der SAT-Protokollierung
MODIFY-SAT-FILTER-CONDITIONS	Änderung der Filterbedingungen
REMOVE-SAT-FILTER-CONDITIONS	Entfernung der Filterbedingungen
SAVE-SAT-PARAMETERS	Speicherung der spezifizierten SAT-Parameter für den nächsten Systemstart
SHOW-SAT-FILTER-CONDITIONS	Anzeige der Filterbedingungen.

**SAT-Protokollierung steuern**

HOLD-SAT-LOGGING	Anhalten der Protokollierung, Schließen der SATLOG-Datei
RESUME-SAT-LOGGING	Fortsetzung der Protokollierung in einer neuen SATLOG-Datei
SHOW-SAT-STATUS	Anzeige des Zustands der SAT-Protokollierung (... INFORMATION=*LOGGING-STATUS)

**SATLOG-Datei**

CHANGE-SAT-FILE	Schließen der aktuellen SATLOG-Datei und Öffnen einer neuen SATLOG-Datei. Während des Wechsels gehen keine Daten verloren.
SAVE-SAT-PARAMETERS	Speicherung der spezifizierten SAT-Parameter für den nächsten Systemstart in einer SAT-Parameter-Datei
SHOW-SAT-STATUS	Anzeige des Dateinamens der SATLOG-Datei, der Datei-Attribute und des aktuellen Protokoll-Status (... INFORMATION=*COLLECTION-FILE)

**SAT-Alarm-Funktion**

ADD-SAT-ALARM-CONDITIONS	Definition von Bedingungen, die eine Konsolmeldung auslösen, um den Sicherheitsbeauftragten von Sicherheitsverstößen sofort in Kenntnis zu setzen
MODIFY-SAT-ALARM-CONDITIONS	Änderung der Alarmbedingungen
REMOVE-SAT-ALARM-CONDITIONS	Entfernung der Alarmbedingungen
SAVE-SAT-PARAMETERS	Speicherung der spezifizierten SAT-Parameter für den nächsten Systemstart
SHOW-SAT-ALARM-CONDITIONS	Anzeige der Alarmbedingungen.

*Hinweise*

In SATCP stehen die Kommandos in unterschiedlichem Umfang zur Verfügung, je nach Zustand der Protokollierung:

<b>SATCP-Status (wie bei Ausgabe von SHOW-SAT-STATUS)</b>			
<b>Kommando</b>	<b>HOLD</b>	<b>RECORD</b>	<b>NO-RESOURCE</b>
HOLD-SAT-LOGGING	-	X	X
RESUME-SAT-LOGGING	X	-	-
MODIFY-SAT-PRESELECTION	-	X	-
SHOW-SAT-STATUS	X	X	X
MODIFY-SAT-SUPPORT-PARAMETERS	-	X	-
SHOW-SAT-SUPPORT-PARAMETERS	X	X	X
CHANGE-SAT-FILE	-	X	-
SAVE-SAT-PARAMETERS	-	X	-
ADD-SAT-ALARM-CONDITIONS	-	X	-
MODIFY-SAT-ALARM-CONDITIONS	-	X	-
REMOVE-SAT-ALARM-CONDITIONS	-	X	-
SHOW-SAT-ALARM-CONDITIONS	X	X	X
ADD-SAT-FILTER-CONDITIONS	-	X	-
MODIFY-SAT-FILTER-CONDITIONS	-	X	-
REMOVE-SAT-FILTER-CONDITIONS	-	X	-
SHOW-SAT-FILTER-CONDITIONS	X	X	X

Alle SAT-Kommandos werden serialisiert, das heißt, ein SAT-Kommando wird abgewiesen, wenn ein anderes Kommando in Bearbeitung ist (Ausnahme: das Kommando /SHOW-SAT-STATUS sowie die Kommandos /SHOW-SAT-ALARM-CONDITIONS, /SHOW-SAT-FILTER-CONDITIONS und /SHOW-SAT-SUPPORT-PARAMETERS jeweils mit Operand VALUE=\*STD/\*CURRENT).

Tritt bei der Ausführung eines SAT-Kommandos ein Fehler auf, wird der Spin-off-Mechanismus ausgelöst.

## **ADD-SAT-ALARM-CONDITIONS**

### **Alarmbedingung definieren**

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit diesem Kommando definiert der Sicherheitsbeauftragte Bedingungen für das Eintreten einer Alarmsituation.

Die Alarmdefinition kann mit dem Kommando /SHOW-SAT-ALARM-CONDITIONS angezeigt und mit /REMOVE-SAT-ALARM-CONDITIONS wieder entfernt werden.

Die alarmlösenden Ereignisse werden wie folgt spezifiziert:

- durch den Ereignisnamen und das Ergebnis beim Eintreten des Ereignisses
- durch die Benutzererkennung des registrierten Ereignisses
- durch die Information zu diesem Ereignis

Tritt eine bestimmte Anzahl derartiger Ereignisse in einem vorgegebenen Zeitraum ein, so wird ein Alarm in Form einer Meldung auf der Operator-Konsole ausgelöst.

**ADD-SAT-ALARM-CONDITIONS**

```

NAME = <name 1..8>
,SELECT = *PARAMETERS(...)
  *PARAMETERS(...)
    EVENT-NAME = *ALL / list-poss(50): <name 3..3>(…)
      <name 3..3>(…)
        | RESULT = *ALL / *SUCCESS / *FAILURE
    ,USER-IDENTIFICATION = *ALL / list-poss(50): <name 1..8>
    ,FIELD-NAME = *ALL / list-poss(50): <name 3..7>(…)
      <name 3..7>(…)
        | VALUE = *ALL / *MATCH(...) / *NOT-MATCH(...) / list-poss(10): <text> /
          list-poss(10): <integer 0..2147483647>(…)
          *MATCH(PATTERN=<text>)
          *NOT-MATCH(PATTERN=<text>)
          <integer 0..2147483647>(…)
            | UNIT = *BYTES / *KB / *MB / *GB
    ,TIME-LIMIT = *UNDEFINED / *WITHIN(...)
      *WITHIN(...)
        | DAYS = <integer 0..365>
        | ,HOURS = <integer 0..23>
        | ,MINUTES = <integer 0..59>
    ,REPEAT = 3 / <integer 1..255>
    ,TRIGGER-ACTION = *OPERATOR-MESSAGE(...)
      *OPERATOR-MESSAGE(...)
        | WAIT-RESPONSE = *YES / *NO

```

**NAME = <name 1..8>**

Name des Alarms.

**SELECT = \*PARAMETERS(...)**

Hier wird definiert, welche Ereignisbedingungen zutreffen müssen, um die Alarmdefinition zu erfüllen.

**EVENT-NAME =**

Art und Resultat der zu überwachenden Ereignisse.

**EVENT-NAME = \*ALL**

Es werden alle von SAT registrierbaren Ereignisse für die Alarm-Funktion überwacht.

**EVENT-NAME = list-poss(50): <name 3..3>(…)**

Expliziter Name eines Ereignisses. Der Name des Ereignisses muss der „[Tabelle der Objekteignisse](#)“ auf Seite 196ff entnommen sein. Bei der Angabe von Ereignissen des Produkts POSIX beachten Sie bitte insbesondere Hinweis [4 auf Seite 66](#).

**RESULT = \*ALL / \*SUCCESS / \*FAILURE**

Spezifiziert welches Ergebnis das Ereignis haben muss.

**USER-IDENTIFICATION =**

Gibt an, welche Benutzerkennungen überwacht werden sollen.

**USER-IDENTIFICATION = \*ALL**

Jede Benutzerkennung wird überwacht.

**USER-IDENTIFICATION = list-poss(50): <name 1..8>**

Die angegebenen Benutzerkennungen werden überwacht. Die Benutzerkennungen müssen zum Zeitpunkt der Definition der Alarmbedingung dem System nicht bekannt sein.

**FIELD-NAME =**

Spezifiziert, welches Datenfeld eines Ereignisses überwacht werden soll.

**FIELD-NAME = \*ALL**

Alle Datenfelder eines Ereignisses werden überwacht.

**FIELD-NAME = list-poss(50): <name 3..7>(…)**

Nur ein hier spezifiziertes Datenfeld wird überwacht. Die Liste der möglichen Feldnamen findet sich in den „[Tabellen der protokollierbaren Information je Objekteignis](#)“ auf Seite 213ff.

**VALUE = \*ALL / \*MATCH(...) / \*NOT-MATCH(...) / list-poss(10): <text> / list-poss(10): <integer 0..2147483647>(…)**

Die Liste der Feldnamen und der dort ausgegebenen Information findet sich in den „[Tabellen der protokollierbaren Information je Objekteignis](#)“ auf Seite 213ff. <text> hängt vom protokollierten Datenfeld ab.

**VALUE = \*MATCH(...)**

Angabe eines Musters für den Feldnamen. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Muster-Angabe im Format <c-string 1..255>, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wildcards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / < > : ,) in einer Zeichenfolge (z.B. ab\\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).
  - s<sub>x</sub> darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
  - s<sub>y</sub> darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
  - s<sub>x</sub> muss in der alphabetischen Sortierung vor s<sub>y</sub> stehen. Ist s<sub>x</sub> kürzer als s<sub>y</sub> wird s<sub>x</sub> mit X'00' aufgefüllt.
  - Ist s<sub>y</sub> kürzer als s<sub>x</sub> wird s<sub>y</sub> mit X'FF' aufgefüllt.
  - Weder in s<sub>x</sub> noch in s<sub>y</sub> dürfen Platzhalter vorkommen.
- <s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe <s<sub>x</sub>:s<sub>y</sub>> sein.

#### **VALUE = \*NOT-MATCH(...)**

Angabe eines Musters für den Feldnamen. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

#### **PATTERN = <text>**

Musterangabe wie bei VALUE=\*MATCH.

**VALUE = <integer 0..2147483647>(…)**

Angabe eines Zahlenwertes für den Feldnamen. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

**UNIT = \*BYTES / \*KB / \*MB / \*GB**

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.
- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
*BYTES	$2^{31}-1 = 2\ 147\ 483\ 647$	$2^{31}-1 = 2\ 147\ 483\ 647$
*KB	$2^{30}-1 = 1\ 073\ 741\ 823$	$2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$
*MB	$2^{20}-1 = 1\ 048\ 575$	$2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$
*GB	$2^{10}-1 = 1\ 023$	$2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$

**TIME-LIMIT =**

Zeitraum, innerhalb das (mit REPEAT festgelegte, x-malige) Auftreten eines Ereignisses zu einem Alarm führt.

**TIME-LIMIT = \*UNDEFINED**

Es wird der gesamte Zeitraum einer SAT-Protokollierung bewertet. Dies bedeutet, dass schon das x-malige Auftreten eines Ereignisses zu einem Alarm führt. Soll z.B. die falsche Eingabe von Kennwörtern überwacht werden, führt im Überwachungszustand TIME-LIMIT=UNDEFINED auch die einmal wöchentlich falsche Eingabe (eventuell wegen Tippfehler) zu einem Alarm. Der Aufmerksamkeitswert des Alarms wird durch diese Art von Meldungen deutlich verringert. Überwachungen über große Zeiträume hinweg sind deshalb angemessener mit der Auswertung von SATLOG-Dateien durchzuführen.

**TIME-LIMIT = \*WITHIN(...)**

Gibt den Zeitraum an, der zwischen dem ersten Auftreten und dem letzten des zu bewertenden Ereignisses liegen darf. Es sind alle drei Operanden mit Parametern zu versorgen.

**DAYS = <integer 0..365>**

Angabe des Zeitraums in Tagen.

**HOURS = <integer 0..23>**

Angabe des Zeitraums in Stunden.

**MINUTES = <integer 0..59>**

Angabe des Zeitraums in Minuten.

**REPEAT= 3 / <integer 1..255>**

Anzahl, wie oft ein Ereignis im definierten Zeitraum eintreten muss, um einen Alarm auszulösen.

**TRIGGER-ACTION = \*OPERATOR-MESSAGE(...)**

Gibt an, welche Aktion ausgeführt werden soll, um den Alarm zu geben und wie darauf geantwortet werden soll. In dieser Version ist nur die Ausgabe einer Meldung (SAT2200) auf die Operator-Konsole möglich.

**WAIT-RESPONSE = \*YES / \*NO**

Gibt an, ob die Meldung bestätigt werden muss oder nicht.

**Kommando-Returncode**

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt Warnung: Benutzer ist unbekannt
	32	SAT0000	Nicht behebbarer Fehler
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	64	SAT1020	Ereignis in Ereignisliste bereits vorhanden
	64	SAT1022	Feld bereits in Feldliste vorhanden
	64	SAT1023	Feld hat doppelte Werte
	64	SAT1026	Angegebenes Zeitlimit ungültig
	64	SAT1027	Alarm bereits vorhanden
	64	SAT1029	Ereignis unbekannt
	64	SAT1030	Benutzer in Benutzerliste bereits vorhanden
	64	SAT1035	Wert ist kein Vielfaches von 512 oder zu groß
	64	SAT1050	Kommando nur erlaubt, wenn Logging-Funktion aktiviert
	64	SAT1071	Alarmtabelle ist voll
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung

*Hinweise*

1. Es gibt keine vordefinierten Alarmdefinitionen. Beim allerersten Start von SAT ist die SAT-Parameter-Datei noch nicht vorhanden; es können aus ihr deshalb auch keine Definitionen gelesen werden.
2. Es ist allerdings möglich, mit dem Kommando /SAVE-SAT-PARAMETERS eine SAT-Parameter-Datei für die nächste Sitzung bereitzustellen. Beim nächsten Start von SAT stehen dann Definitionen mit den Standard-Werten zur Verfügung. Für Alarmdefinitionen gibt es keine Standard-Werte. Werden in der SAT-Parameter-Datei nicht die aktuellen Werte gespeichert, werden für die nächste Sitzung keine Alarmdefinitionen übernommen.
3. Es können maximal 32 Alarmdefinitionen hinterlegt werden.
4. Enthält eine Alarmdefinition ein Ereignis eines Produkts, für das die Aktivierung des SAT-Supports mit /MODIFY-SAT-SUPPORT-PARAMETERS gesteuert werden kann (in der aktuellen Version ist dies nur das Produkt POSIX), so kann dieser Alarm bei Auftreten des Ereignisses nur ausgelöst werden, wenn für das betreffende Produkt der SAT-Support aktiviert ist.
5. Für die Auswertung einer Alarmbedingung mit UNIT-Angabe ist grundsätzlich nur der Wert von Belang, der sich aus der Multiplikation der VALUE- und der UNIT-Angabe ergibt, nicht jedoch, wie dieser Wert zustande kommt.

*Beispiele*

Die folgenden Angaben werden als gleichwertig betrachtet, da jede denselben Wert von 3145728 Bytes darstellt:

```
VALUE=3145728(UNIT=*BYTES)
VALUE=3072(UNIT=*KB)
VALUE=3(UNIT=*MB)
```

- a) Ein ADD-SAT-ALARM-CONDITIONS-Kommando mit der Angabe

```
FIELD-NAME=*FILPOS(VALUE=(3072(UNIT=*KB),3(UNIT=*MB)))
```

wird daher mit folgender Meldung zurückgewiesen:

```
SAT1023 FIELD 'FILPOS' CONTAINS DUPLICATE VALUES. COMMAND REJECTED
```

- b) Eine Alarmbedingung mit der Angabe

```
FIELD-NAME=*FILPOS(VALUE=3072(UNIT=*KB))
```

trifft zu, wenn der zu protokollierende Satz `FILPOS=6144` enthält. Grund: Die Angabe im Satz stellt ein Vielfaches von 512 Bytes dar (siehe „[filpos](#)“ auf [Seite 285](#)) und  $6144 \cdot 512$  Bytes = 3145728 Bytes = 3072 KB.

6. Posix-filenames und Kerberos-Namen werden von SAT ohne Einschränkung protokolliert. Bei der Definition von SAT-Alarmen wird die Groß- und Kleinschreibung bei folgenden SAT-Feldern unterstützt: AUDITID, HOMEDIR, LINKNAM, NEWPATH, PATHNAM, PRINCCL, PRINCSV, SHELL, SYMBDEV. Die Felder können mit Ausnahme von SYMBDEV allerdings nur in einer Länge von max. 255 Bytes angegeben werden. Events mit längeren Feldinhalten können durch die Angabe von Wildcards selektiert werden. Für die Angabe eines Einzelnamens (ohne Wildcards) werden Sonderzeichen zugelassen, wie sie für posix-filenames bzw. für Kerberos-Namen erlaubt sind.
7. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

Jeder fehlerhafte Versuch, sich an der Station DSN30151 unter der Kennung SYSPRIV anzumelden, soll zu einem Alarm führen (für das Beispiel wird angenommen, dass die angegebene Station meistens vom Sicherheitsbeauftragten verwendet wird):

```
/add-sat-alarm-conditions name=badlogon,select=*parameters( -  
/                               event-name=jde(result=*failure), -  
/                               user-identification=syspriv, -  
/                               field=station(value='dsn30151')),repeat=1
```

## ADD-SAT-FILTER-CONDITIONS

### Filterbedingung definieren

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit diesem Kommando definiert der Sicherheitsbeauftragte Bedingungen zur Vorauswahl der SAT-Protokollierung.

Die Filterdefinition kann mit dem Kommando /SHOW-SAT-FILTER-CONDITIONS angezeigt und mit /REMOVE-SAT-FILTER-CONDITIONS wieder entfernt werden.

Wenn für ein Ereignis eine Vorauswahl möglich ist, wird diese Bedingung mit herangezogen, um zu entscheiden, ob das Ereignis protokolliert werden soll oder nicht.

Die zur Entscheidungsfindung benutzten Ereignisse sind wie folgt festgelegt:

- durch den Ereignisnamen und das Ergebnis beim Eintreten des Ereignisses.
- durch die Benutzerkennung des registrierten Ereignisses.
- durch die Information zu diesem Ereignis.

#### *Hinweise*

- Protokollsätze, auf die keine Filterbedingung zutrifft, werden aufgezeichnet.
- Falls auf einen Protokollsatz eine einzige Filterbedingung zutrifft, so gilt die in dieser Bedingung festgelegte Aktion.
- Wenn auf einen Protokollsatz mehrere Filterbedingungen gleichzeitig zutreffen, so sind die beiden folgenden Fälle zu unterscheiden:
  1. Falls mindestens eine der zutreffenden Filterbedingungen im Operanden TRIGGER-ACTION die Angabe \*LOGGING(RECORDING=\*YES) enthält, wird der Protokollsatz aufgezeichnet.
  2. Nur wenn **alle** zutreffenden Filterbedingungen im Operanden TRIGGER-ACTION die Angabe \*LOGGING(RECORDING=\*NO) enthalten, wird der Protokollsatz nicht aufgezeichnet.

**ADD-SAT-FILTER-CONDITIONS**

```

NAME = <name 1..8>
, SELECT = *PARAMETERS(...)
  *PARAMETERS(...)
    EVENT-NAME = *ALL / list-poss(50): <name 3..3>(…)
      <name 3..3>(…)
        | RESULT = *ALL / *SUCCESS / *FAILURE
    , USER-IDENTIFICATION = *ALL / list-poss(50): <name 1..8>
    , FIELD-NAME = *ALL / list-poss(50): <name 3..7>(…)
      <name 3..7>(…)
        | VALUE = *ALL / *MATCH(…) / *NOT-MATCH(…) / list-poss(10): <text> /
          list-poss(10): <integer 0..2147483647>(…)
            *MATCH(PATTERN=<text>)
            *NOT-MATCH(PATTERN=<text>)
            <integer 0..2147483647>(…)
              | UNIT = *BYTES / *KB / *MB / *GB
    , TRIGGER-ACTION = *LOGGING(…)
      *LOGGING(…)
        | RECORDING = *YES / *NO

```

**NAME = <name 1..8>**

Name des Filters.

**SELECT = \*PARAMETERS(…)**

Hier wird festgelegt, welche Ereignisse die Filterbedingung erfüllen.

**EVENT-NAME =**

Art und Resultat der Ereignisse, die die Filterbedingung erfüllen.

**EVENT-NAME = \*ALL**

Alle von SAT registrierbaren Ereignisse erfüllen die Filterbedingung.

**EVENT-NAME = list-poss(50): <name 3..3>(…)**Expliziter Name eines Ereignisses. Der Name des Ereignisses muss der „[Tabelle der Objekteignisse](#)“ auf Seite 196ff entnommen sein.**RESULT = \*ALL / \*SUCCESS / \*FAILURE**

Spezifiziert welches Ergebnis das Ereignis haben muss.

**USER-IDENTIFICATION =**

Gibt an, welche Benutzerkennungen die Filterbedingung erfüllen.

**USER-IDENTIFICATION = \*ALL**

Jede Benutzerkennung erfüllt die Filterbedingung.

**USER-IDENTIFICATION = list-poss(50): <name 1..8>**

Nur Ereignisse, die die angegebenen Benutzerkennungen betreffen, erfüllen die Filterbedingung. Die Benutzerkennungen müssen zum Zeitpunkt der Definition der Filterbedingung dem System nicht bekannt sein.

**FIELD-NAME =**

Spezifiziert, welches Datenfeld eines Ereignisses geprüft werden soll.

**FIELD-NAME = \*ALL**

Alle Datenfelder eines Ereignisses werden geprüft.

**FIELD-NAME = list-poss(50): <name 3..7>(…)**

Nur ein hier spezifiziertes Datenfeld wird geprüft. Die Liste der möglichen Feldnamen findet sich in der „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf [Seite 213ff.](#)

**VALUE = \*ALL / \*MATCH(...) / \*NOT-MATCH(...) / list-poss(10): <text> / list-poss(10): <integer 0..2147483647>(…)**

Die Liste der Feldnamen und der dort ausgegebenen Information findet sich in den „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf [Seite 213ff.](#) <text> hängt vom protokollierten Datenfeld ab.

**VALUE = \*MATCH(...)**

Angabe eines Musters für den Feldnamen. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Muster-Angabe im Format <c-string 1..255>, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wildcards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / < > : ,) in einer Zeichenfolge (z.B. ab\\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).
  - s<sub>x</sub> darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
  - s<sub>y</sub> darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
  - s<sub>x</sub> muss in der alphabetischen Sortierung vor s<sub>y</sub> stehen. Ist s<sub>x</sub> kürzer als s<sub>y</sub> wird s<sub>x</sub> mit X'00' aufgefüllt.
  - Ist s<sub>y</sub> kürzer als s<sub>x</sub> wird s<sub>y</sub> mit X'FF' aufgefüllt.
  - Weder in s<sub>x</sub> noch in s<sub>y</sub> dürfen Platzhalter vorkommen.
- <s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe <s<sub>x</sub>:s<sub>y</sub>> sein.

#### **VALUE = \*NOT-MATCH(...)**

Angabe eines Musters für den Feldnamen. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

#### **PATTERN = <text>**

Musterangabe wie bei VALUE=\*MATCH.

**VALUE = <integer 0..2147483647>(…)**

Angabe eines Zahlenwertes für den Feldnamen. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

**UNIT = \*BYTES / \*KB / \*MB / \*GB**

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.
- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
*BYTES	$2^{31}-1 = 2\ 147\ 483\ 647$	$2^{31}-1 = 2\ 147\ 483\ 647$
*KB	$2^{30}-1 = 1\ 073\ 741\ 823$	$2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$
*MB	$2^{20}-1 = 1\ 048\ 575$	$2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$
*GB	$2^{10}-1 = 1\ 023$	$2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$

**TRIGGER-ACTION = \*LOGGING(…)**

Gibt an, welche Aktion ausgeführt werden soll, wenn die mit dem Operanden SELECT festgelegte Bedingung erfüllt ist.

**RECORDING =**

Angabe, ob ein Ereignis protokolliert werden soll.

**RECORDING = \*YES**

Das Ereignis wird protokolliert.

**RECORDING = \*NO**

Das Ereignis wird nicht protokolliert, sofern keine andere Filterbedingung die Protokollierung verlangt.

**Kommando-Returncode**

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt Warnung: Benutzer ist unbekannt
	32	SAT0000	Nicht behebbarer Fehler
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	64	SAT1020	Ereignis in Ereignisliste bereits vorhanden
	64	SAT1022	Feld bereits in Feldliste vorhanden
	64	SAT1023	Feld hat doppelte Werte
	64	SAT1029	Ereignis unbekannt
	64	SAT1030	Benutzer in Benutzerliste bereits vorhanden
	64	SAT1031	Filter bereits vorhanden
	64	SAT1035	Wert ist kein Vielfaches von 512 oder zu groß
	64	SAT1050	Kommando nur erlaubt, wenn Logging-Funktion aktiviert
	64	SAT1073	Filtertabelle ist voll
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung

*Hinweise*

1. Es gibt keine vordefinierten Filterdefinitionen. Beim allerersten Start von SAT ist die SAT-Parameter-Datei noch nicht vorhanden; es können aus ihr deshalb auch keine Definitionen gelesen werden.
2. Es ist allerdings möglich, mit dem Kommando /SAVE-SAT-PARAMETERS eine SAT-Parameter-Datei für die nächste Sitzung bereitzustellen. Beim nächsten Start von SAT stehen dann Definitionen mit den Standard-Werten zur Verfügung. Für Filterdefinitionen gibt es keine Standard-Werte. Werden in der SAT-Parameter-Datei nicht die aktuellen Werte gespeichert, werden für die nächste Sitzung keine Filterdefinitionen übernommen.
3. Es können maximal 32 Filterdefinitionen hinterlegt werden.
4. Die Verwendung einer Negativliste von Feldnamen und die Trigger-Action RECORDING=\*YES führt meist nicht zur Verringerung des Aufzeichnungsumfang, da in einem Protokollsatz meist Felder enthalten sind, die dann ein Aufzeichnen anfordern.

5. Für die Auswertung einer Filterbedingung mit UNIT-Angabe ist grundsätzlich nur der Wert von Belang, der sich aus der Multiplikation der VALUE- und der UNIT-Angabe ergibt, nicht jedoch wie dieser Wert zustande kommt.

### *Beispiele*

Die folgenden Angaben werden als gleichwertig betrachtet, da jede denselben Wert von 3145728 Bytes darstellt:

```
VALUE=3145728(UNIT=*BYTES)
```

```
VALUE=3072(UNIT=*KB)
```

```
VALUE=3(UNIT=*MB)
```

- a) Ein ADD-SAT-FILTER-CONDITIONS-Kommando mit der Angabe

```
FIELD-NAME=*FILPOS(VALUE=(3072(UNIT=*KB),3(UNIT=*MB)))
```

wird daher mit folgender Meldung zurückgewiesen:

```
SAT1023 FIELD 'FILPOS' CONTAINS DUPLICATE VALUES. COMMAND REJECTED
```

- b) Eine Filterbedingung mit der Angabe

```
FIELD-NAME=*FILPOS(VALUE=3072(UNIT=*KB))
```

trifft zu, wenn der zu protokollierende Satz `FILPOS=6144` enthält. Grund: Die Angabe im Satz stellt ein Vielfaches von 512 Bytes dar (siehe „[filpos](#)“ auf [Seite 285](#)) und  $6144 \cdot 512 \text{ Bytes} = 3145728 \text{ Bytes} = 3072 \text{ KB}$ .

6. Posix-filenames und Kerberos-Namen werden von SAT ohne Einschränkung protokolliert. Bei der Definition von SAT-Filtern wird die Groß- und Kleinschreibung bei folgenden SAT-Feldern unterstützt: AUDITID, HOMEDIR, LINKNAM, NEWPATH, PATHNAM, PRINCCL, PRINCSV, SHELL, SYMBDEV. Die Felder können mit Ausnahme von SYMBDEV allerdings nur in einer Länge von max. 255 Bytes angegeben werden. Events mit längeren Feldinhalten können durch die Angabe von Wildcards selektiert werden. Für die Angabe eines Einzelnamens (ohne Wildcards) werden Sonderzeichen zugelassen, wie sie für posix-filenames bzw. für Kerberos-Namen erlaubt sind.
7. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

1. Folgende Zugriffe sollen aufgezeichnet werden, falls sie auf Dateien erfolgen, die im Katalog „CAT1“ katalogisiert sind und deren Name die Zeichenfolgen „SYS“ und „ABC“ enthält: „Lesen der Schutzattribute“ (FRS), falls erfolgreich, und „Katalog exportieren“ (CEP)

```
/add-sat-filter-conditions name=filter1,select=*parameters( -
/   event-name=(frs,cep),trigger-action=*logging(recording=*no)
/add-sat-filter-conditions name=filter2,select=*parameters( -
/   event-name=(frs(result=*success),cep),user-identification=*all,-
/   field-name=(filename(value=*match(pattern='*sys*abc')), -
/               catid(value='cat1')))
```

2. Die Zugriffe auf die Dateien, deren Name mit „\$TSOS.SYSLNK.“ beginnt, sollen nicht aufgezeichnet werden.

```
/add-sat-filter-conditions name=f1,select=*parameters( -
/   event-name=*all,user-identification=*all,-
/   field-name=filename(value=*match(pattern='*$tsos.syslnk.*')), -
/   trigger-action=*logging(recording=*no)
```

Das Ereignis „Datei-Löschen“ (FDD) soll aber für alle Dateien aufgezeichnet werden:

```
/add-sat-filter-conditions name=f2,select=*parameters( -
/   event-name=fdd,user-identification=*all,field-name=*all), -
/   trigger-action=*logging(recording=*yes)
```

Für das Löschen einer Datei, deren Name mit \$TSOS.SYSLNK. beginnt, treffen beide Bedingungen zu. Da in einer dieser Bedingungen die Aufzeichnung verlangt wird, wird der entsprechende Protokollsatz aufgezeichnet.

Weitere Beispiele finden Sie bei /MODIFY-SAT-FILTER-CONDITIONS.

## CHANGE-SAT-FILE

### SATLOG-Datei wechseln

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION, SAT-FILE-MANAGEMENT

Mit dem Kommando /CHANGE-SAT-FILE schließt der SAT-Datei-Verwalter die aktuelle SATLOG-Datei und eröffnet eine neue SATLOG-Datei im laufenden Betrieb. Während des Wechsels gehen keine Daten verloren. Für die neue SAT-Protokoll-Datei können neue Attribute vergeben werden.

Der Sicherheitsbeauftragte kann mit diesem Kommando ebenfalls die SATLOG-Datei wechseln, er darf jedoch nur die Standardwerte der Operanden verwenden.

CHANGE-SAT-FILE
<pre> <b>BUFFER-LENGTH</b> = <u>*UNCHANGED</u> / *STD(...)   *STD(...)       <b>SIZE</b> = <u>2</u> / &lt;integer 1..16&gt; <b>,SPACE</b> = <u>*UNCHANGED</u> / *RELATIVE(...)   *RELATIVE(...)       <b>PRIMARY-ALLOCATION</b> = <u>120</u> / &lt;integer 6..50331645&gt;       <b>,SECONDARY-ALLOCATION</b> = <u>120</u> / &lt;integer 2..32767&gt; <b>,SUPPORT</b> = <u>*PUBLIC</u> / *PRIVATE-VOLUME(...)   *PRIVATE-VOLUME(...)       <b>VOLUME</b> = &lt;vsn 1..6&gt;       <b>,DEVICE-TYPE</b> = &lt;structured-name 1..8&gt; <b>,REPEAT</b> = <u>*UNCHANGED</u> / *NO / *PERIOD(...)   *PERIOD(...)       <b>DAYS</b> = <u>1</u> / &lt;integer 0..10&gt;       <b>,HOURS</b> = <u>0</u> / &lt;integer 0..23&gt; </pre>

#### **BUFFER-LENGTH =**

Bestimmt die Puffergröße der SATLOG-Datei.

#### **BUFFER-LENGTH = \*UNCHANGED**

Die Puffergröße bleibt unverändert.

**BUFFER-LENGTH = \*STD(...)**

Bestimmt eine neue Puffergröße. Standard-Wert ist 2 PAM pages. Ein kleiner Wert für BUFFER-LENGTH stellt sicher, dass die Ein-/ Ausgaberate erhöht wird und bei einer abnormen Systembeendigung ein Minimum an Daten verlorenght.

**SIZE = 2 / <integer 1..16>**

Bestimmt die Puffergröße. Standard-Wert ist 2 PAM pages.

**SPACE =**

Legt die Speicherplatzzuordnung fest.

**SPACE = \*UNCHANGED**

Die Speicherplatzzuordnung bleibt unverändert.

**SPACE = \*RELATIVE(...)**

Bestimmt die Größe der Primär- und Sekundärzuweisung.

**PRIMARY-ALLOCATION = 120 / <integer 6..50331645>**

Primärzuweisung

**SECONDARY-ALLOCATION = 120 / <integer 2..32767>**

Sekundärzuweisung

Werden viele Ereignisse aufgezeichnet, muss die Sekundärzuweisung groß sein. Sie kann klein sein, wenn die Standard-Werte auf einer kleinen Anlage verwendet werden.

**SUPPORT =**

Bestimmt, auf welchen Plattenspeichern die SATLOG-Dateien erstellt werden. Die Zuweisung gilt nur für die aktuelle Datei.

**SUPPORT = \*PUBLIC**

Die SATLOG-Dateien werden auf gemeinschaftlichen Plattenspeichern erstellt. Die erste SATLOG-Datei eines Systemlaufs wird immer auf einem gemeinschaftlichen Plattenspeicher erstellt.

**SUPPORT = \*PRIVATE-VOLUME(...)**

Die SATLOG-Dateien werden auf privaten Plattenspeichern erstellt.

**VOLUME = <vsn 1..6>**

Archivnummer.

**DEVICE-TYPE = <structured-name 1..8>**

Gerätetyp.

**REPEAT = \*UNCHANGED / \*NO / \*PERIOD(...)**

Bestimmt, ob die SATLOG-Datei periodisch gewechselt werden soll.

**REPEAT = \*NO**

Die SATLOG-Datei wird nicht periodisch gewechselt.

**REPEAT = \*PERIOD(...)**

Die SATLOG-Datei wird periodisch gewechselt.

**DAYS=1 / <integer 0..10>**

Angabe für den periodischen Wechsel in Tagen.

**HOURS = 0 / <integer 0..23>**

Angabe für den periodischen Wechsel in Stunden.

**Kommando-Returncode**

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt Warnung: Periodisches Wechseln abgewiesen
	32	SAT0000	Nicht behebbarer Fehler
	32	SAT2030	DVS-Fehler beim Öffnen der Datei
	32	SAT2040	DVS-Fehler beim Anlegen des Katalogeintrags
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	64	SAT1025	Falsche Zeitangabe für periodischen Wechsel
	64	SAT1050	Kommando nur erlaubt, wenn Logging-Funktion aktiviert
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung

*Hinweise*

1. Alle Einstellungen sind so lange gültig, bis sie mit einem erneuten Kommando /CHANGE-SAT-FILE geändert werden oder bis SHUTDOWN.
2. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

Die SAT-Datei-Verwaltung will

- die SATLOG-Datei wechseln (explizites Umschalten)
- die neue SATLOG-Datei auf dem privaten Plattenspeicher PRV003 erstellen:

```
/change-sat-file support=*private-volume(volume=prv003,device=d3435)
```

oder in Kurzform:

```
/cha-sat-file sup=*priv-vol(prv003,d3435)
```

## HOLD-SAT-LOGGING

### Protokollierung anhalten

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /HOLD-SAT-LOGGING hält der Sicherheitsbeauftragte die SAT-Protokollierung und Alarm-Funktion an und schließt die aktuelle SATLOG-Datei. SATCP befindet sich dann im HOLD-Zustand. Im HOLD-Zustand stehen nicht alle Kommandos zur Verfügung (siehe [Seite 59](#)).

<b>HOLD-SAT-LOGGING</b>

Dieses Kommando hat keine Operanden.

#### Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	SAT0000	Nicht behebbarer Fehler
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung
	128	SAT2010	Logging-Funktion bereits in Hold-Zustand

#### Hinweise

1. Wenn SATCP im Zustand NO-RESOURCE ist, können Benutzeraufträge, die auf eine Protokollierung warten, nach Eingabe von HOLD-SAT-LOGGING wieder weiterlaufen.

Falls im Klasse-5-Speicher noch SATLOG-Sätze der wartenden Aufträge gepuffert sind, ist anschließend die Eingabe des Kommandos RESUME-SAT-LOGGING erforderlich, um die Verarbeitung dieser Aufträge fortzusetzen.

Solange die Verarbeitung der wartenden Aufträge noch nicht durch das Kommando RESUME-SAT-LOGGING fortgesetzt wurde, gibt SATCP in regelmäßigen Abständen eine Meldung aus, die anzeigt, dass noch wartende Aufträge existieren.

2. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

## MODIFY-SAT-ALARM-CONDITIONS

### Alarmdefinition ändern

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /MODIFY-SAT-ALARM-CONDITIONS kann eine bestehende Alarmdefinition (/ADD-SAT-ALARM-CONDITIONS) geändert werden.

#### MODIFY-SAT-ALARM-CONDITIONS

**NAME** = <name 1..8>

,**SELECT** = \*PARAMETERS(...)

\*PARAMETERS(...)

**EVENT-NAME** = \*UNCHANGED / \*ALL / list-poss(50): <name 3..3>(…)

        <name 3..3>(…)

**SELECT-SWITCH** = \*ON(…)/ \*OFF

                \*ON(…)

**RESULT** = \*ALL / \*SUCCESS / \*FAILURE

    ,**USER-IDENTIFICATION** = \*UNCHANGED / \*ALL / list-poss(50): <name 1..8>(…)

        <name 1..8>(…)

**SELECT-SWITCH** = \*ON / \*OFF

(Teil 1 von 2)

```

, FIELD-NAME = *UNCHANGED / *ALL / list-poss(50): <name 3..7>(…)
  <name 3..7>(…)
    SELECT-SWITCH = *ON(…) / *OFF(…)
      *ON(…)
        VALUE = *ALL / *MATCH(…) / *NOT-MATCH(…) / list-poss(10): <text> /
          list-poss(10): <integer 0..2147483647>(…)
            *MATCH(PATTERN=<text>)
            *NOT-MATCH(PATTERN=<text>)
            <integer 0..2147483647>(…)
              | UNIT = *BYTES / *KB / *MB / *GB
      *OFF(…)
        VALUE = *ALL / *MATCH(…) / *NOT-MATCH(…) / list-poss(10): <text> /
          list-poss(10): <integer 0..2147483647>(…)
            *MATCH(PATTERN=<text>)
            *NOT-MATCH(PATTERN=<text>)
            <integer 0..2147483647>(…)
              | UNIT = *BYTES / *KB / *MB / *GB
, TIME-LIMIT = *UNCHANGED / *UNDEFINED / *WITHIN(…)
  *WITHIN(…)
    | DAYS = <integer 0..365>
    | HOURS = <integer 0..23>
    | MINUTES = <integer 0..59>
, REPEAT = *UNCHANGED / <integer 1..255>
, TRIGGER-ACTION = *UNCHANGED / *OPERATOR-MESSAGE(…)
  *OPERATOR-MESSAGE(…)
    | WAIT-RESPONSE = *YES / *NO

```

(Teil 2 von 2)

**NAME** = <name 1..8>

Name des Alarms.

**SELECT** = \*PARAMETERS(…)

Definiert, welche der bestehenden Bedingungen geändert werden sollen.

**EVENT-NAME** = \*UNCHANGED / \***ALL** / list-poss(50): <name 3..3>(…)

Art und Resultat der zu überwachenden Ereignisse.

**EVENT-NAME = \*ALL**

Es werden alle von SAT registrierbaren Ereignisse für die Alarm-Funktion überwacht.

**EVENT-NAME = list-poss(50): <name 3..3>(…)**

Expliziter Name eines Ereignisses. Der Name des Ereignisses muss der „[Tabelle der Objekteignisse](#)“ auf Seite 196ff entnommen sein. Bei der Angabe von Ereignissen des Produkts POSIX beachten Sie bitte insbesondere Hinweis [6 auf Seite 90](#).

**SELECT-SWITCH =**

Spezifiziert, ob das Ereignis hinzugefügt oder entfernt werden soll.

**SELECT-SWITCH = \*ON(…)**

Ereignis und Ergebnis werden zu der Alarmdefinition hinzugefügt.

**RESULT = \*ALL / \*SUCCESS / \*FAILURE**

Spezifiziert, welches Ergebnis das Ereignis haben muss.

**SELECT-SWITCH = \*OFF**

Das Ereignis wird aus der Alarmdefinition entfernt.

**USER-IDENTIFICATION = \*UNCHANGED / \*ALL / list-poss(50): <name 1..8>(…)**

Gibt an, welche Benutzerkennungen überwacht werden sollen.

**USER-IDENTIFICATION = \*ALL**

Jede Benutzerkennung wird überwacht.

**USER-IDENTIFICATION = list-poss(50): <name 1..8>(…)**

Die angegebenen Benutzerkennungen werden überwacht. Die Benutzerkennung muss zum Zeitpunkt der Definition der Alarmbedingung dem System nicht bekannt sein.

**SELECT-SWITCH =**

Spezifiziert, ob die Benutzerkennung hinzugefügt oder entfernt werden soll.

**SELECT-SWITCH = \*ON**

Die Kennung wird zur Alarmdefinition hinzugefügt.

**SELECT-SWITCH = \*OFF**

Die Kennung wird aus der Alarmdefinition entfernt.

**FIELD-NAME = \*UNCHANGED / \*ALL / list-poss(50): <name 3..7>(…)**

Spezifiziert, welches Datenfeld eines Ereignisses überwacht werden soll.

**FIELD-NAME = \*ALL**

Alle Datenfelder eines Ereignisses werden überwacht.

**FIELD-NAME = list-poss(50): <name 3..7>(…)**

Es wird ein Datenfeld spezifiziert. Die Tabelle der möglichen Feldnamen findet sich in den „[Tabellen der protokollierbaren Information je Objekteignis](#)“ auf Seite 213ff.

**SELECT-SWITCH =**

Zu überwachende Informationen werden der Definition hinzugefügt oder aus ihr entfernt, wenn sie einen mit dem Operanden VALUE festgelegten Wert haben. Die Tabelle der Feldnamen und der dort ausgegebenen Information findet sich in der „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213ff.

<text> hängt vom protokollierten Datenfeld ab.

**SELECT-SWITCH = \*ON(...)**

Fügt zu überwachende Informationen der Alarmdefinition hinzu.

**VALUE = \*ALL**

Jede Information wird überwacht.

**VALUE = \*MATCH(...)**

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Muster-Angabe im Format c-string 1..255, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wild-cards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / > : ,) in einer Zeichenfolge (z.B. ab\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).

- $s_x$  darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
  - $s_y$  darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
  - $s_x$  muss in der alphabetischen Sortierung vor  $s_y$  stehen. Ist  $s_x$  kürzer als  $s_y$  wird  $s_x$  mit X'00' aufgefüllt.
  - Ist  $s_y$  kürzer als  $s_x$  wird  $s_y$  mit X'FF' aufgefüllt.
  - Weder in  $s_x$  noch in  $s_y$  dürfen Platzhalter vorkommen.
- <s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe < $s_x$ ; $s_y$ > sein.

**VALUE = \*NOT-MATCH(...)**

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Musterangabe wie bei VALUE=\*MATCH.

**VALUE = list-poss(10): <text>**

Die explizit angegebene Information für das Feld wird überwacht. <text> hängt vom protokollierten Datenfeld ab. Die Tabelle der Feldnamen und der dort ausgegebenen Information findet sich in der „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213ff.

**VALUE = list-poss(10): <integer 0..2147483647>(…)**

Die explizit in Form eines Zahlenwertes angegebene Information für das Feld wird überwacht. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

**UNIT = \*BYTES / \*KB / \*MB / \*GB**

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.

- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
*BYTES	$2^{31}-1 = 2\ 147\ 483\ 647$	$2^{31}-1 = 2\ 147\ 483\ 647$
*KB	$2^{30}-1 = 1\ 073\ 741\ 823$	$2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$
*MB	$2^{20}-1 = 1\ 048\ 575$	$2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$
*GB	$2^{10}-1 = 1\ 023$	$2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$

### SELECT-SWITCH = \*OFF(...)

Entfernt zu überwachende Information aus der Alarmdefinition.

#### VALUE = \*ALL

Jede Information wird entfernt.

#### VALUE = \*MATCH(...)

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

#### PATTERN = <text>

Muster-Angabe im Format c-string 1..255, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wild-cards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / < > : .) in einer Zeichenfolge (z.B. ab\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).

- $s_x$  darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
- $s_y$  darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
- $s_x$  muss in der alphabetischen Sortierung vor  $s_y$  stehen. Ist  $s_x$  kürzer als  $s_y$  wird  $s_x$  mit X'00' aufgefüllt.
- Ist  $s_y$  kürzer als  $s_x$  wird  $s_y$  mit X'FF' aufgefüllt.
- Weder in  $s_x$  noch in  $s_y$  dürfen Platzhalter vorkommen.

<s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe < $s_x$ ; $s_y$ > sein.

#### VALUE = \*NOT-MATCH(...)

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

#### PATTERN = <text>

Musterangabe wie bei VALUE=\*MATCH.

#### VALUE = list-poss(10): <text>

Die explizit angegebene Information für das Feld wird aus der Alarmdefinition entfernt. <text> hängt vom protokollierten Datenfeld ab. Die Tabelle der Feldnamen und der dort ausgegebenen Information findet sich in der „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213ff.

#### VALUE = list-poss(10): <integer 0..2147483647>(…)

Die explizit in Form eines Zahlenwertes angegebene Information für das Feld wird aus der Alarmdefinition entfernt. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

#### UNIT = \*BYTES / \*KB / \*MB / \*GB

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.

- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
*BYTES	$2^{31}-1 = 2\,147\,483\,647$	$2^{31}-1 = 2\,147\,483\,647$
*KB	$2^{30}-1 = 1\,073\,741\,823$	$2^{40}-2^{10} = 1\,099\,511\,626\,752$
*MB	$2^{20}-1 = 1\,048\,575$	$2^{40}-2^{20} = 1\,099\,510\,579\,200$
*GB	$2^{10}-1 = 1\,023$	$2^{40}-2^{30} = 1\,098\,437\,885\,952$

**TIME-LIMIT = \*UNCHANGED / \*UNDEFINED / \*WITHIN(...)**

Zeitraum, innerhalb dem das (mit REPEAT festgelegte, x-malige) Auftreten eines Ereignisses zu einem Alarm führt.

**TIME-LIMIT = \*UNDEFINED**

Es wird der gesamte Zeitraum einer SAT-Protokollierung bewertet. Dies bedeutet, dass schon das x-malige Auftreten eines Ereignisses zu einem Alarm führt. Soll z.B. die falsche Eingabe von Kennwörtern überwacht werden, führt im Überwachungszustand TIME-LIMIT=\*UNDEFINED auch die einmal wöchentlich falsche Eingabe (eventuell wegen Tippfehler) zu einem Alarm. Der Aufmerksamkeitswert des Alarms wird durch diese Art von Meldungen deutlich verringert. Überwachungen über große Zeiträume hinweg sind deshalb angemessener mit der Auswertung von SATLOG-Dateien durchzuführen.

**TIME-LIMIT = \*WITHIN(...)**

Gibt den Zeitraum an, der zwischen dem ersten Auftreten und dem letzten des zu bewertenden Ereignisses liegen darf. Es sind alle drei Operanden mit Parametern zu versorgen.

**DAYS = <integer 0..365>**

Angabe des Zeitraums in Tagen.

**HOURS = <integer 0..23>**

Angabe des Zeitraums in Stunden.

**MINUTES = <integer 0..59>**

Angabe des Zeitraums in Minuten.

**REPEAT= \*UNCHANGED / <integer 1..255>**

Anzahl, wie oft ein Ereignis im definierten Zeitraum eintreten muss, um einen Alarm auszulösen.

**TRIGGER-ACTION = \*UNCHANGED / \*OPERATOR-MESSAGE(...)**

Gibt an, welche Aktion ausgeführt werden soll, um den Alarm zu geben und wie darauf geantwortet werden soll. In dieser Version ist nur die Ausgabe einer Meldung (SAT2200) auf die Operator-Konsole möglich.

**TRIGGER-ACTION = \*OPERATOR-MESSAGE(...)**

Gibt an, wie auf die Ausgabe der Meldung reagiert werden muss.

**WAIT-RESPONSE = \*YES / \*NO**

Gibt an, ob die Meldung bestätigt werden muss oder nicht.

**Kommando-Returncode**

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt Warnung: Benutzer unbekannt Warnung: Alarm nicht ausgelöst Warnung: Mehr als eine Warnung ausgegeben
	32	SAT 0000	Nicht behebbarer Fehler
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	64	SAT1020	Ereignis in Ereignisliste bereits vorhanden
	64	SAT1022	Feld bereits in Feldliste vorhanden
	64	SAT1023	Feld hat doppelte Werte
	64	SAT1026	Angegebenes Zeitlimit ungültig
	64	SAT1028	Alarm unbekannt
	64	SAT1029	Ereignis unbekannt
	64	SAT1030	Benutzer in Benutzerliste bereits vorhanden
	64	SAT1035	Wert ist kein Vielfaches von 512 oder zu groß
	64	SAT1050	Kommando nur erlaubt, wenn Logging-Funktion aktiviert
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung

*Hinweise*

1. Bei der Verwendung von Mustern für Werte eines Feldes wird nicht geprüft, ob es zu Überschneidungen kommt.
2. Identische Musterangaben für einen Wert eines Feldes werden ersetzt.

*Beispiele*

Eine Alarmbedingung sei folgendermaßen definiert:

```
/add-sat-alarm-conditions name=alarm1, ... -
/      field-name=filename(value=*match('*abc*')), ...
```

## a) Das Kommando

```
/modify-sat-alarm-conditions name=alarm1, ... -
/      field-name=filename( -
/      select-switch=*on(value=*not-match('*abc*')), ...
```

überschreibt das Vergleichsmuster. Die Wirkung ist so, als ob die Bedingung auf folgende Weise festgelegt worden wäre:

```
/add-sat-alarm-conditions name=alarm1, ... -
/      field-name=filename(value=*not-match('*abc*')), ...
```

- b) Sowohl die Angabe `SELECT-SWITCH=*OFF(VALUE=*MATCH('*ABC*'))` als auch `SELECT-SWITCH=*OFF(VALUE=*NOT-MATCH('*ABC*'))` entfernen `*MATCH('*ABC*')` aus der Werteliste.

3. Die Angabe eines festen Wertes hat keinen Einfluss auf eine Musterangabe.

Beispielsweise hat ein `/MODIFY-SAT-ALARM-CONDITIONS`-Kommando mit der Angabe `VALUE='XABCY'` keinen Einfluss auf eine Alarmbedingung, die mit `VALUE=*MATCH('*ABC*')` festgelegt wurde. Der Wert `'XABCY'` ist bereits in der Musterangabe `'*ABC*'` enthalten, die Bedingung `VALUE='XABCY'` ist also automatisch erfüllt, wenn `*MATCH='*ABC*'` erfüllt ist.

Auf eine Alarmbedingung, die mit `VALUE=*NOT-MATCH('*ABC*')` festgelegt wurde, hat die Angabe `VALUE='XABCY'` jedoch Einfluss. In diesem Fall gilt die Bedingung für alle Werte, die nicht in das Muster `'*ABC*'` passen, und zusätzlich für den Wert `'XABCY'`.

4. SELECT-SWITCH=\*OFF entfernt die angegebenen Objekte aus einer Liste, die mit SELECT-SWITCH=\*ON oder einem entsprechenden /ADD-SAT-ALARM-CONDITIONS-Kommando definiert wurde. Falls \*ALL gültig ist, wird das Objekt in eine Negativliste aufgenommen.

Die Angaben zum Operanden SELECT-SWITCH (in allen Fällen) werden nur berücksichtigt, wenn dadurch Bedingungen entstehen. Wurde beispielsweise mit dem Kommando /ADD-SAT-ALARM-CONDITIONS für einen Alarm USER-ID=\*ALL festgelegt, so hat die Angabe USER-ID=HUGO(SELECT-SWITCH=\*ON) im Kommando /MODIFY-SAT-ALARM-CONDITIONS keine Wirkung. Die Angabe USER-ID=HUGO(SELECT-SWITCH=\*OFF) bewirkt einen Eintrag dieses Wertes in eine Negativliste.

5. Ist für einen Feldwert ein Muster gültig, kann durch SELECT-SWITCH=\*OFF(VALUE=wert) keine Teilmenge aus dem Muster herausgelöst werden: Wenn z.B. eine Alarmbedingung mit SELECT-SWITCH=\*ON(VALUE=\*MATCH(\*ABC\*)) oder einem entsprechenden /ADD-SAT-ALARM-CONDITIONS-Kommando festgelegt wurde, ist ein /MODIFY-SAT-ALARM-CONDITIONS-Kommando mit der Angabe SELECT-SWITCH=\*OFF(VALUE='SYSABC') wirkungslos.

#### *Beispiel*

Eine Alarmbedingung sei auf folgende Weise definiert:

```
/add-sat-alarm-conditions name=alarm1, -
/      field-name=filename(value=*match('*abc*')), ...
```

Das Kommando

```
/modify-sat-alarm-conditions name=alarm1, ... -
/  field-name=filename( -
/      select-switch=*off(value=:cati:$tsos.sysabc))
```

hat keine Wirkung.

6. Enthält eine Alarmdefinition ein Ereignis eines Produkts, für das die Aktivierung des SAT-Supports mit /MODIFY-SAT-SUPPORT-PARAMETERS gesteuert werden kann (in der aktuellen Version ist dies nur das Produkt POSIX), so kann dieser Alarm bei Auftreten des Ereignisses nur ausgelöst werden, wenn für das betreffende Produkt der SAT-Support aktiviert ist.

7. Für die Auswertung einer Alarmbedingung mit UNIT-Angabe ist grundsätzlich nur der Wert von Belang, der sich aus der Multiplikation der VALUE- und der UNIT-Angabe ergibt, nicht jedoch wie dieser Wert zustande kommt.

### Beispiele

Die folgenden Angaben werden als gleichwertig betrachtet, da jede denselben Wert von 3145728 Bytes darstellt:

```
VALUE=3145728(UNIT=*BYTES)
```

```
VALUE=3072(UNIT=*KB)
```

```
VALUE=3(UNIT=*MB)
```

- a) Ein MODIFY-SAT-ALARM-CONDITIONS-Kommando mit der Angabe

```
FIELD-NAME=*FILPOS(SELECT-SWITCH=*ON(
    VALUE=(3072(UNIT=*KB),3(UNIT=*MB))))
```

wird daher mit folgender Meldung zurückgewiesen:

```
SAT1023 FIELD 'FILPOS' CONTAINS DUPLICATE VALUES. COMMAND REJECTED
```

- b) Eine Alarmbedingung, die mit der Angabe VALUE=3145728(UNIT=\*BYTES) in einem ADD-SAT-ALARM-CONDITIONS-Kommando gesetzt wurde, kann mit der Angabe VALUE=3(UNIT=\*MB) in einem MODIFY-SAT-ALARM-CONDITIONS-Kommando wieder aus der Alarmtabelle entfernt werden.

- c) Eine Alarmbedingung mit der Angabe

```
FIELD-NAME=*FILPOS(SELECT-SWITCH=*ON(VALUE=3072(UNIT=*KB)))
```

trifft zu, wenn der zu protokollierende Satz FILPOS=6144 enthält. Grund: Die Angabe im Satz stellt ein Vielfaches von 512 Bytes dar (siehe „[filpos](#)“ auf [Seite 285](#)) und  $6144 \cdot 512 \text{ Bytes} = 3145728 \text{ Bytes} = 3072 \text{ KB}$ .

8. Posix-filenames und Kerberos-Namen werden von SAT ohne Einschränkung protokolliert. Bei der Definition von SAT-Alarmen wird die Groß- und Kleinschreibung bei folgenden SAT-Feldern unterstützt: AUDITID, HOMEDIR, LINKNAM, NEWPATH, PATHNAM, PRINCCL, PRINCSV, SHELL, SYMBDEV. Die Felder können mit Ausnahme von SYMBDEV allerdings nur in einer Länge von max. 255 Bytes angegeben werden. Events mit längeren Feldinhalten können durch die Angabe von Wildcards selektiert werden. Für die Angabe eines Einzelnamens (ohne Wildcards) werden Sonderzeichen zugelassen, wie sie für posix-filenames bzw. für Kerberos-Namen erlaubt sind.
9. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

Im Beispiel zu /ADD-SAT-ALARM-CONDITIONS wurde ein Alarm mit dem Namen badlogon definiert. Dieser Alarm wird durch jeden fehlerhaften Versuch, sich an der Station DSN30151 unter der Benutzerkennung SYSPRIV anzumelden, ausgelöst:

```
/add-sat-alarm-conditions name=badlogon,select=*parameters( -  
/      event-name=jde(result=*failure), -  
/      user-identification=syspriv, -  
/      field=station(value='dsn30151')),repeat=1
```

Dieser Alarm soll nun so geändert werden, dass jeder fehlerhafte Versuch, sich unter der Benutzerkennung SYSPRIV, zu einem Alarm führt, unabhängig von der Station, an der er erfolgt. Die Alarmdefinition wird wie folgt geändert:

```
/modify-sat-alarm-conditions name=badlogon,select=*parameters( -  
/      field-name=station(select-switch=*on(value=*all)))
```

## MODIFY-SAT-FILTER-CONDITIONS

### Filterdefinition ändern

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /MODIFY-SAT-FILTER-CONDITIONS kann eine bestehende Filterdefinition (/ADD-FILTER-CONDITIONS) geändert werden.

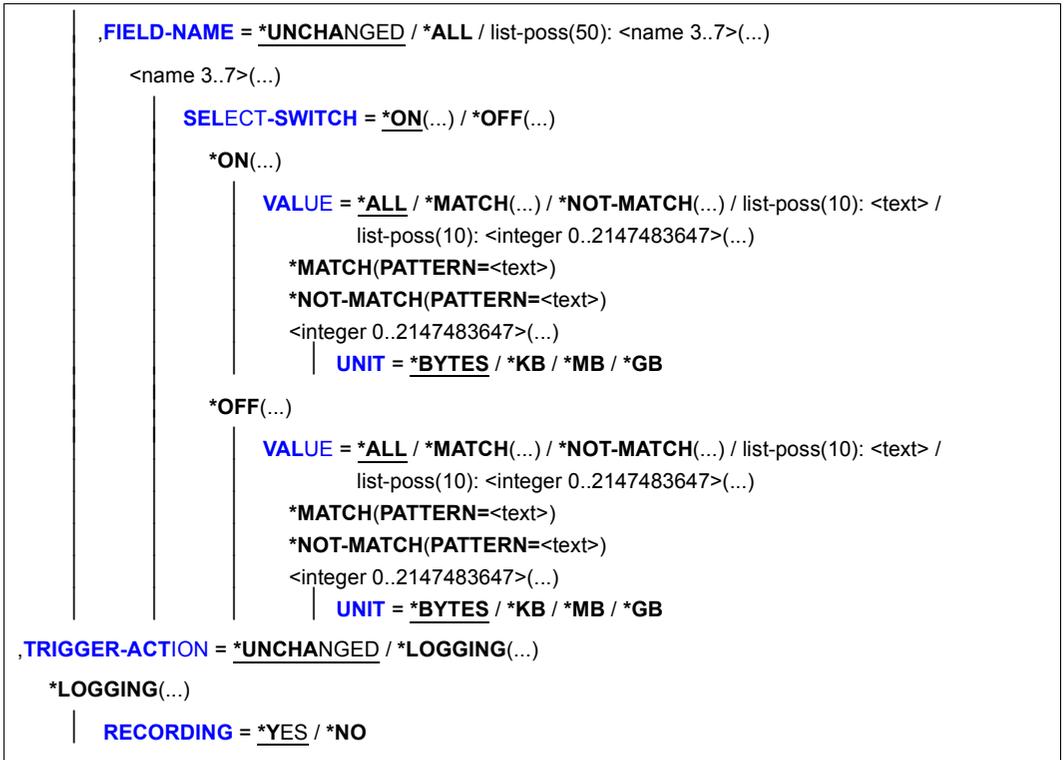
#### MODIFY-SAT-FILTER-CONDITIONS

```

NAME = <name 1..8>
, SELECT = *PARAMETERS(...)
  *PARAMETERS(...)
    | EVENT-NAME = *UNCHANGED / *ALL / list-poss(50): <name 3..3>(…)
    | <name 3..3>(…)
    | | SELECT-SWITCH = *ON(…) / *OFF
    | | | *ON(…)
    | | | | RESULT = *ALL / *SUCCESS / *FAILURE
    | , USER-IDENTIFICATION = *UNCHANGED / *ALL / list-poss(50): <name 1..8>(…)
    | <name 1..8>(…)
    | | SELECT-SWITCH = *ON / *OFF

```

(Teil 1 von 2)



(Teil 2 von 2)

**NAME** = <name 1..8>

Name des Filters.

**SELECT** = \*PARAMETERS(…)

Definiert, welche der bestehenden Bedingungen geändert werden sollen.

**EVENT-NAME** = \*UNCHANGED / \*ALL / list-poss(50): <name 3..3>(…)

Art und Resultat der Ereignisse, die die Filterbedingung erfüllen.

**EVENT-NAME** = \*ALL

Alle von SAT registrierbaren Ereignisse erfüllen die Filterbedingung.

**EVENT-NAME = list-poss(50): <name 3..3>(…)**

Expliziter Name eines Ereignisses. Der Name des Ereignisses muss der „[Tabelle der Objekteignisse](#)“ auf Seite 196ff entnommen sein.

**SELECT-SWITCH =**

Spezifiziert, ob das Ereignis hinzugefügt oder entfernt werden soll.

**SELECT-SWITCH = \*ON(…)**

Ereignis und Ergebnis werden zu der Filterdefinition hinzugefügt.

**RESULT = \*ALL / \*SUCCESS / \*FAILURE**

Spezifiziert, welches Ergebnis das Ereignis haben muss.

**SELECT-SWITCH = \*OFF**

Das Ereignis wird aus der Filterdefinition entfernt.

**USER-IDENTIFICATION = \*UNCHANGED / \*ALL / list-poss(50): <name 1..8>(…)**

Gibt an, welche Benutzerkennungen die Filterbedingung erfüllen.

**USER-IDENTIFICATION = \*ALL**

Jede Benutzerkennung erfüllt die Filterbedingung.

**USER-IDENTIFICATION = list-poss(50): <name 1..8>(…)**

Nur Ereignisse, die die angegebenen Benutzerkennungen betreffen, erfüllen die Filterbedingung. Die Benutzerkennungen müssen zum Zeitpunkt der Definition der Filterbedingung dem System nicht bekannt sein.

**SELECT-SWITCH =**

Spezifiziert, ob die Benutzerkennung hinzugefügt oder entfernt werden soll.

**SELECT-SWITCH = \*ON**

Die Kennung wird zur Filterdefinition hinzugefügt.

**SELECT-SWITCH = \*OFF**

Die Kennung wird aus der Filterdefinition entfernt.

**FIELD-NAME = \*UNCHANGED / \*ALL / list-poss(50): <name 3..7>(…)**

Spezifiziert, welches Datenfeld eines Ereignisses geprüft werden soll. Die Tabelle der möglichen Feldnamen findet sich in der „[Tabellen der protokollierbaren Information je Objekteignis](#)“ auf Seite 213ff.

**FIELD-NAME = \*ALL**

Alle Datenfelder eines Ereignisses erfüllen die Filterbedingung.

**FIELD-NAME = list-poss(50): <name 3..7>(…)**

Es wird ein Datenfeld spezifiziert.

**SELECT-SWITCH =**

Ereignisse werden der Definition hinzugefügt oder aus ihr entfernt, wenn die zugehörige Information einen mit dem Operanden VALUE festgelegten Wert hat. Die Tabelle der Feldnamen und der dort ausgegebenen Information findet sich in der „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213ff. <text> hängt vom protokollierten Datenfeld ab.

**SELECT-SWITCH = \*ON(...)**

Fügt zu prüfende Informationen der Filterdefinition hinzu.

**VALUE = \*ALL**

Jede Information erfüllt die Filterbedingung.

**VALUE = \*MATCH(...)**

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Muster-Angabe im Format c-string 1..255, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wild-cards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / > : ,) in einer Zeichenfolge (z.B. ab\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).

- $s_x$  darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
  - $s_y$  darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
  - $s_x$  muss in der alphabetischen Sortierung vor  $s_y$  stehen. Ist  $s_x$  kürzer als  $s_y$  wird  $s_x$  mit X'00' aufgefüllt.
  - Ist  $s_y$  kürzer als  $s_x$  wird  $s_y$  mit X'FF' aufgefüllt.
  - Weder in  $s_x$  noch in  $s_y$  dürfen Platzhalter vorkommen.
- <s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe < $s_x$ : $s_y$ > sein.

**VALUE = \*NOT-MATCH(...)**

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Musterangabe wie bei VALUE=\*MATCH.

**VALUE = list-poss(10):<text>**

Die explizit angegebene Information für das Feld erfüllt die Filterbedingung.

**VALUE = list-poss(10): <integer 0..2147483647>(…)**

Die explizit in Form eines Zahlenwertes angegebene Information für das Feld erfüllt die Filterbedingung. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

**UNIT = \*BYTES / \*KB / \*MB / \*GB**

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.

- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
*BYTES	$2^{31}-1 = 2\ 147\ 483\ 647$	$2^{31}-1 = 2\ 147\ 483\ 647$
*KB	$2^{30}-1 = 1\ 073\ 741\ 823$	$2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$
*MB	$2^{20}-1 = 1\ 048\ 575$	$2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$
*GB	$2^{10}-1 = 1\ 023$	$2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$

### SELECT-SWITCH = \*OFF(...)

Entfernt Ereignisse aus der Filterdefinition.

#### VALUE = \*ALL

Jede Information wird aus der Filterdefinition entfernt.

#### VALUE = \*MATCH(...)

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

#### PATTERN = <text>

Muster-Angabe im Format c-string 1..255, wobei analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wild-cards) ersetzt werden können.

Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / < > : .) in einer Zeichenfolge (z.B. ab\\*c bezeichnet die Zeichenfolge „ab\*c“).
- <s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:
  - Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
  - Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).

- $s_x$  darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
  - $s_y$  darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
  - $s_x$  muss in der alphabetischen Sortierung vor  $s_y$  stehen. Ist  $s_x$  kürzer als  $s_y$  wird  $s_x$  mit X'00' aufgefüllt.
  - Ist  $s_y$  kürzer als  $s_x$  wird  $s_y$  mit X'FF' aufgefüllt.
  - Weder in  $s_x$  noch in  $s_y$  dürfen Platzhalter vorkommen.
- <s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe < $s_x$ ; $s_y$ > sein.

**VALUE = \*NOT-MATCH(...)**

Angabe eines Musters für die Information. Die Bedingung ist gültig, wenn der Vergleichswert **nicht** in dieses Muster passt. Die Muster-Angabe ist nur für Feldnamen erlaubt, deren Werte eine Zeichenkette darstellen (<c-string>, <filename>, <name>).

**PATTERN = <text>**

Musterangabe wie bei VALUE=\*MATCH.

**VALUE = list-poss(10): <text>**

Die explizit angegebene Information für das Feld wird aus der Filterdefinition entfernt.

**VALUE = list-poss(10): <integer 0..2147483647>(…)**

Die explizit in Form eines Zahlenwertes angegebene Information für das Feld wird aus der Filterdefinition entfernt. Diese Angabe ist nur für Feldnamen erlaubt, deren Werte vom Typ <integer> sind.

**UNIT = \*BYTES / \*KB / \*MB / \*GB**

Angabe der Maßeinheit, in der die mit dem Operanden VALUE vorgenommene Wertangabe zu interpretieren ist. Diese Angabe ist nur für die Feldnamen filpos, curlim2 und maxlim2 erlaubt.

Dabei gilt Folgendes:

- Falls implizit oder explizit UNIT=\*BYTES festgelegt ist, muss der Wert ein Vielfaches von 512 sein.

- Der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes darf auch nicht überschritten werden, wenn UNIT=\*KB / \*MB / \*GB angegeben ist. Damit ergeben sich abhängig von der UNIT-Angabe folgende Maximalwerte:

UNIT=	Maximalwert bei VALUE	entspricht in Bytes
<b>*BYTES</b>	$2^{31}-1 = 2\ 147\ 483\ 647$	$2^{31}-1 = 2\ 147\ 483\ 647$
<b>*KB</b>	$2^{30}-1 = 1\ 073\ 741\ 823$	$2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$
<b>*MB</b>	$2^{20}-1 = 1\ 048\ 575$	$2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$
<b>*GB</b>	$2^{10}-1 = 1\ 023$	$2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$

**TRIGGER-ACTION = \*UNCHANGED / \*LOGGING(...)**

Gibt an, welche Aktion ausgeführt werden soll, wenn die mit dem Operanden SELECT festgelegte Bedingung erfüllt ist.

**TRIGGER-ACTION = \*LOGGING(...)**

Angabe, ob ein Ereignis protokolliert werden soll.

**RECORDING = \*YES**

Das Ereignis wird protokolliert.

**RECORDING = \*NO**

Das Ereignis wird nicht protokolliert, sofern keine andere Filterbedingung die Protokollierung verlangt.

**Kommando-Returncode**

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt Warnung: Benutzer unbekannt Warnung: Filter nicht wirksam
	32	SAT 0000	Nicht behebbarer Fehler
	64	SAT1000	Benutzer für Kommando nicht privilegiert
	64	SAT1020	Ereignis in Ereignisliste bereits vorhanden
	64	SAT1022	Feld bereits in Feldliste vorhanden
	64	SAT1023	Feld hat doppelte Werte
	64	SAT1029	Ereignis unbekannt
	64	SAT1030	Benutzer in Benutzerliste bereits vorhanden
	64	SAT1031	Filter unbekannt
	64	SAT1035	Wert ist kein Vielfaches von 512 oder zu groß
	64	SAT1050	Kommando nur erlaubt, wenn Logging-Funktion aktiviert
	128	SAT1010	Anderes Kommando wird derzeit ausgeführt
	128	SAT1080	Wechsel in Vorbereitung

*Hinweise*

1. Bei der Verwendung von Mustern für Werte eines Feldes wird nicht geprüft, ob es zu Überschneidungen kommt.
2. Identische Musterangaben für einen Wert eines Feldes werden ersetzt.

*Beispiele*

Eine Filterbedingung sei folgendermaßen definiert:

```
/add-sat-filter-conditions name=filter1, ... -
/      field-name=filename(value=*match('*abc*')), ...
```

a) Das Kommando

```
/modify-sat-filter-conditions name=filter1, ... -
/  field-name=filename( -
/    select-switch=*on(value=*not-match('*abc*'))), ...
```

überschreibt das Vergleichsmuster. Die Wirkung ist so, als ob die Bedingung auf folgende Weise festgelegt worden wäre:

```
/add-sat-filter-conditions name=filter1, ... -
/      field-name=filename(value=*not-match('*abc*')), ...
```

- b) Sowohl die Angabe `SELECT-SWITCH=*OFF(VALUE=*MATCH('*ABC*'))` als auch `SELECT-SWITCH=*OFF(VALUE=*NOT-MATCH('*ABC*'))` entfernen `*MATCH('*ABC*')` aus der Werteliste.

3. Die Angabe eines festen Wertes hat keinen Einfluss auf eine Musterangabe.

Beispielsweise hat ein /MODIFY-SAT-FILTER-CONDITIONS-Kommando mit der Angabe VALUE='XABCY' keinen Einfluss auf eine Filterbedingung, die mit VALUE=\*MATCH(\*ABC\*) festgelegt wurde. Der Wert 'XABCY' ist bereits in der Musterangabe '\*ABC\*' enthalten, die Bedingung VALUE='XABCY' ist also automatisch erfüllt, wenn \*MATCH=\*ABC\* erfüllt ist.

Auf eine Filterbedingung, die mit VALUE=\*NOT-MATCH(\*ABC\*) festgelegt wurde, hat die Angabe VALUE='XABCY' jedoch Einfluss. In diesem Fall gilt die Bedingung für alle Werte, die nicht in das Muster '\*ABC\*' passen, und zusätzlich für den Wert 'XABCY'.

4. SELECT-SWITCH=\*OFF entfernt die angegebenen Objekte aus einer Liste, die mit SELECT-SWITCH=\*ON oder einem entsprechenden /ADD-SAT-FILTER-CONDITIONS-Kommando definiert wurde. Falls \*ALL gültig ist, wird das Objekt in eine Negativliste aufgenommen.

Die Angaben zum Operanden SELECT-SWITCH (in allen Fällen) werden nur berücksichtigt, wenn dadurch Bedingungen entstehen. Wurde beispielsweise mit dem Kommando /ADD-SAT-FILTER-CONDITIONS für einen Filter USER-ID=\*ALL festgelegt, so hat die Angabe USER-ID=HUGO(SELECT-SWITCH=\*ON) im Kommando /MODIFY-SAT-FILTER-CONDITIONS keine Wirkung. Die Angabe USER-ID=HUGO(SELECT-SWITCH=\*OFF) bewirkt einen Eintrag dieses Wertes in eine Negativliste.

5. Ist für einen Feldwert ein Muster gültig, kann durch SELECT-SWITCH=\*OFF(VALUE=wert) keine Teilmenge aus dem Muster herausgelöst werden: Wenn z.B. eine Filterbedingung mit SELECT-SWITCH=\*ON(VALUE=\*MATCH(\*ABC\*)) oder einem entsprechenden /ADD-SAT-FILTER-CONDITIONS-Kommando festgelegt wurde, ist ein /MODIFY-SAT-FILTER-CONDITIONS-Kommando mit der Angabe SELECT-SWITCH=\*OFF(VALUE='SYSABC') wirkungslos. Der gewünschte Effekt kann jedoch durch die Definition einer zweiten Filterbedingung erzielt werden:

#### *Beispiel*

Eine Filterbedingung sei auf folgende Weise definiert:

```
/add-sat-filter-conditions name=filter1, -
/      field-name=filename(value=*match(*abc*)), -
/      trigger-action=*logging(recording=*no), ...
```

- a) Das Kommando

```
/modify-sat-filter-conditions name=filter1, ... -
/  field-name=filename( -
/      select-switch=*off(value=:cati:$tsos.sysabc))
```

hat keine Wirkung.

## b) Die Definition einer zweiten Filterbedingung

```
/add-sat-filter-conditions name=filter2, -
/ field-name=filename(value=:cati:$tsos.sysabc), ...
/ trigger-action=*logging(recording=*yes)
```

bewirkt folgendes:

Auf Protokollsätze, die die Datei :CATI:\$TSOS.SYSABC betreffen, treffen beide Filterbedingungen zu. Da eine der beiden Bedingungen (FILTER2) die Protokollierung verlangt, werden die Sätze aufgezeichnet. Protokollsätze, die andere Dateien betreffen, deren Name „ABC“ enthält, werden nicht aufgezeichnet. Auf sie trifft nur die Bedingung FILTER1 zu, die die Protokollierung ausschließt.

6. Für die Auswertung einer Filterbedingung mit UNIT-Angabe ist grundsätzlich nur der Wert von Belang, der sich aus der Multiplikation der VALUE- und der UNIT-Angabe ergibt, nicht jedoch wie dieser Wert zustande kommt.

*Beispiele*

Die folgenden Angaben werden als gleichwertig betrachtet, da jede denselben Wert von 3145728 Bytes darstellt:

```
VALUE=3145728(UNIT=*BYTES)
VALUE=3072(UNIT=*KB)
VALUE=3(UNIT=*MB)
```

- a) Ein MODIFY-SAT-FILTER-CONDITIONS-Kommando mit der Angabe

```
FIELD-NAME=*FILPOS(SELECT-SWITCH=*ON(
VALUE=(3072(UNIT=*KB),3(UNIT=*MB))))
```

wird daher mit folgender Meldung zurückgewiesen:

```
SAT1023 FIELD 'FILPOS' CONTAINS DUPLICATE VALUES. COMMAND REJECTED
```

- b) Eine Filterbedingung, die mit der Angabe VALUE=3145728(UNIT=\*BYTES) in einem ADD-SAT-FILTER-CONDITIONS-Kommando gesetzt wurde, kann mit der Angabe VALUE=3(UNIT=\*MB) in einem MODIFY-SAT-FILTER-CONDITIONS-Kommando wieder aus der Filtertabelle entfernt werden.
- c) Eine Filterbedingung mit der Angabe
- ```
FIELD-NAME=*FILPOS(SELECT-SWITCH=*ON(VALUE=3072(UNIT=*KB)))
```
- trifft zu, wenn der zu protokollierende Satz FILPOS=6144 enthält. Grund: Die Angabe im Satz stellt ein Vielfaches von 512 Bytes dar (siehe „[filpos](#)“ auf [Seite 285](#)) und  $6144 \cdot 512 \text{ Bytes} = 3145728 \text{ Bytes} = 3072 \text{ KB}$ .

7. Posix-filenames und Kerberos-Namen werden von SAT ohne Einschränkung protokolliert. Bei der Definition von SAT-Filtern wird die Groß- und Kleinschreibung bei folgenden SAT-Feldern unterstützt: AUDITID, HOMEDIR, LINKNAM, NEWPATH, PATHNAM, PRINCCL, PRINCSV, SHELL, SYMBDEV. Die Felder können mit Ausnahme von SYMBDEV allerdings nur in einer Länge von max. 255 Bytes angegeben werden. Events mit längeren Feldinhalten können durch die Angabe von Wildcards selektiert werden. Für die Angabe eines Einzelnamens (ohne Wildcards) werden Sonderzeichen zugelassen, wie sie für posix-filenames bzw. für Kerberos-Namen erlaubt sind.
8. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

### *Beispiele*

1. Die Zugriffe auf die Dateien :A:\$TSOS.SYSABC und :B:\$SYS.SYSXXX sollen nur dann aufgezeichnet werden, wenn sie von den Benutzern PAUL und HUGO erfolgen. Zur Definition des dazu erforderlichen Filters werden zwei Kommandos benötigt:

Zunächst muss eine Filterbedingung festgelegt werden, mit der alle Zugriffe auf die beiden Dateien von der Protokollierung ausgeschlossen werden.

```
/add-sat-filter-conditions name=filter1,select=*parameters( -
/   event-name=*all,user-identification=*all, -
/   field-name=filename(value=(a:$tsos.sysabc,b:$sys.sysxxx)), -
/   trigger-action=*logging(*recording = *no)
```

Anschließend muss die Filterbedingung so modifiziert werden, dass sie auf die Benutzer PAUL und HUGO nicht zutrifft, deren Zugriffe somit protokolliert werden.

```
/modify-sat-filter-conditions name=filter1,select=*parameters( -
/   user-id=(paul(select-switch=*off),hugo(select-switch=*off))
```

2. Zugriffe auf Dateien, sollen nur aufgezeichnet werden, wenn im Dateinamen die Zeichenfolge „SYS“ oder „ABC“ vorkommt. Außerdem sollen Zugriffe auf die Datei :A:\$TSOS.SRMLNK aufgezeichnet werden.

Folgende Bedingung schließt die Zugriffe auf die Dateien, deren Name nicht „SYS“ enthält, von der Protokollierung aus:

```
/add-sat-filter-conditions name=f1,select=parameters( -
/   event-name=*all,user-identification= *all, -
/   field-name=filename(value=*not-match(pattern='*sys*')), -
/   trigger-action=*logging(recording=*no)
```

Somit würden nur noch Zugriffe auf Dateien aufgezeichnet, deren Name die Zeichenfolge „SYS“ enthält.

Eine zweite Bedingung verlangt die Protokollierung für die Datei :A:\$TSOS.SRMLNK.

```
/add-sat-filter-conditions name=f2, select=parameters( -
/   field=filename(value=:a:$tsos.srmlnk), -
/   trigger-action = *logging (recording = *yes)
```

Diese Bedingung wird modifiziert, so dass sie auch für Dateien gilt, deren Name „ABC“ enthält:

```
/modify-sat-filter-conditions name=f2, select=parameters( -
/   field-name=filename(select-switch=*on(value=*match('*abc*'))))
```

Für Dateien, deren Name nicht „SYS“, aber „ABC“ enthält, treffen beide Filterbedingungen zu. Da in einer dieser Bedingungen die Protokollierung verlangt wird, wird der Zugriff protokolliert.

## MODIFY-SAT-PRESELECTION

### Auswahl treffen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /MODIFY-SAT-PRESELECTION kann der Sicherheitsbeauftragte Folgendes verändern:

1. die Standard-Werte der Auswahl, mit denen bestimmt wird, ob SATCP ein Ereignis aufzeichnet oder nicht. Die Protokollierung ist abhängig vom Ergebnis der Operation, dem Ereignis-Typ und der Benutzerkennung
2. die Verknüpfungsregel (siehe [Abschnitt „Subjekt, Objekt und Ereignis“ auf Seite 16](#))
3. die Erlaubnis für den Aufruf des System-Exit. Der Exit wird nur aktiviert, wenn die Exit-Routine von der Systemverwaltung geladen ist.
4. den Aufzeichnungsumfang, mit dem festgelegt wird, ob \*EXTENDED-Felder aufgezeichnet werden. \*EXTENDED-Felder sind im [Abschnitt „Tabellen der protokollierbaren Information je Objekt ereignis“ auf Seite 213](#) mit „E“ gekennzeichnet
5. den Standardwert der Protokolliereinstellung („user audit default“) für neu eingerichtete Benutzerkennungen.

Unabhängig vom Kommando /MODIFY-SAT-PRESELECTION kann eine Veränderung des Audit-Eintrags im Katalog die Auswahl von Dateien und Bibliothekselementen beeinflussen.

**MODIFY-SAT-PRESELECTION**

```

EVENT-AUDITING = *UNCHANGED / list-poss(50): <name 3..3>(…)
  <name 3..3>(…)
    | AUDIT-SWITCH = *ON(…) / *OFF
      | *ON(…)
        | RESULT = *ALL / *SUCCESS / *FAILURE
,USER-AUDITING = *UNCHANGED / *ALL-SWITCHABLE(…) / *DEFAULT(…) /
  list-poss(50): <name 1..8>(…)
    *ALL-SWITCHABLE(…)
      | AUDIT-SWITCH = *ON / *OFF
    *DEFAULT(…)
      | NEW-USER = *ON / *OFF
    <name 1..8>(…)
      | AUDIT-SWITCH = *ON / *OFF
,PRESELECTION-RULE = *UNCHANGED / *INDEPENDENT / *FILES-BY-EVENTS
,EXIT = *UNCHANGED / *YES / *NO
,LOGGING-QUANTITY = *UNCHANGED / *STD / *EXTENDED

```

**EVENT-AUDITING =**

Bestimmt die Ereignisse, für die die Protokollierung ein- oder ausgeschaltet wird.

**EVENT-AUDITING = \*UNCHANGED**

Die aktuell gültige Einstellung für die Protokollierung der Ereignisse bleibt unverändert.

**EVENT-AUDITING = list-poss(50): <name 3..3>(…)**

Ereignis, für das die Protokollierung ein- oder ausgeschaltet wird. Die Eingabe besteht aus dem 3-stelligen Kurznamen der Ereignisse, z.B. FCD, FRD,... (siehe „[Tabelle der Objekteignisse](#)“ auf Seite 196ff). Bei der Angabe von Ereignissen des Produkts POSIX beachten Sie bitte insbesondere Hinweis [4 auf Seite 111](#).

**AUDIT-SWITCH =**

Bestimmt, welche Ereignisse protokolliert werden.

**AUDIT-SWITCH = \*ON(...)**

Das betreffende Ereignis wird für die Protokollierung ausgewählt.

**RESULT =**

Bestimmt, in welchem Fall das Ereignis protokolliert werden muss:

**RESULT = \*ALL**

In jedem Fall

**RESULT = \*SUCCESS**

Im Fall einer erfolgreichen Operation

**RESULT = \*FAILURE**

Im Fall einer nicht erfolgreichen Operation

**AUDIT-SWITCH = \*OFF**

Das betreffende Ereignis wird nicht für die Protokollierung ausgewählt.

**USER-AUDITING =**

Bestimmt die Benutzerkennungen, für die die Protokollier-Einstellung verändert wird. Der neue Wert für die Protokollierung einer Benutzerkennung wird in den Benutzerkatalog eingetragen und ist sofort wirksam.

**USER-AUDITING = \*UNCHANGED**

Die aktuell gültige Auswahl der Benutzerkennungen für die Protokollierung bleibt unverändert.

**USER-AUDITING = \*ALL-SWITCHABLE(...)**

Legt für alle schaltbaren Benutzerkennungen fest, welche Ereignisse protokolliert werden. Schaltbare Benutzerkennungen sind alle Benutzerkennungen außer der Kennung des Sicherheitsbeauftragten, der Kennung SYSAUDIT und Benutzerkennungen mit dem Privileg SAT-Datei-Verwaltung.

**AUDIT-SWITCH = \*ON / \*OFF**

Bestimmt, welche Ereignisse protokolliert werden.

**AUDIT-SWITCH = \*ON**

Alle Ereignisse, die von einer schaltbaren Benutzerkennung ausgelöst wurden, werden protokolliert.

**AUDIT-SWITCH = \*OFF**

Ereignisse, die von einer schaltbaren Benutzerkennung ausgelöst wurden, werden nur dann protokolliert, wenn sie mit dem Operanden EVENT-AUDITING ausgewählt wurden und/oder ein ausgewähltes Dateiojekt betreffen (abhängig von der mit dem Operanden PRESELECTION-RULE festgelegten Verknüpfungsregel).

**USER-AUDITING = \*DEFAULT(...)**

Legt den Defaultwert für die Protokolliereinstellung neu eingerichteter Benutzerkennungen fest. Neu eingerichtete Benutzerkennungen sind alle Benutzerkennungen, die nach der Ausführung des aktuellen Kommandos /MODIFY-SAT-PRESELECTION eingerichtet werden.

**NEW-USER = \*ON / \*OFF**

Bestimmt, welche Ereignisse protokolliert werden.

**NEW-USER = \*ON**

Alle Ereignisse, die von einer neu eingerichteten Benutzerkennung ausgelöst wurden, werden protokolliert.

**NEW-USER = \*OFF**

Ereignisse, die von einer neu eingerichteten Benutzerkennung ausgelöst wurden, werden nur dann protokolliert, wenn sie mit dem Operanden EVENT-AUDITING ausgewählt wurden und/oder ein ausgewähltes Dateiojekt betreffen (abhängig von der mit dem Operanden PRESELECTION-RULE festgelegten Verknüpfungsregel).

**USER-AUDITING = list-poss(50): <name 1..8>(…)**

Legt pro angegebener Benutzerkennung fest, welche Ereignisse protokolliert werden.

**AUDIT-SWITCH = \*ON / \*OFF**

Bestimmt, welche Ereignisse protokolliert werden.

**AUDIT-SWITCH = \*ON**

Alle Ereignisse, die von der betreffenden Benutzerkennung ausgelöst wurden, werden protokolliert.



In Systemen mit BS2000 OSD/BC > V11.0A gilt:

Mit dieser Angabe kann die Protokollierung auch für nicht schaltbare Benutzerkennungen eingeschaltet werden, wenn sie aufgrund eines Fehlers ausgeschaltet ist.

**AUDIT-SWITCH = \*OFF**

Ereignisse, die von der betreffenden Benutzerkennung ausgelöst wurden, werden nur dann protokolliert, wenn sie mit dem Operanden EVENT-AUDITING ausgewählt wurden und/oder ein ausgewähltes Dateiojekt betreffen (abhängig von der mit dem Operanden PRESELECTION-RULE festgelegten Verknüpfungsregel).

**PRESELECTION-RULE =**

Bestimmt die Verknüpfungsregel.

**PRESELECTION-RULE = \*UNCHANGED**

Die aktuell gültige Auswahl-Regel bleibt gültig.

**PRESELECTION-RULE = \*INDEPENDENT**

erzwingt die Protokollierung eines Ereignisses, wenn entweder Ereignis oder Subjekt (Benutzerkennung) oder Dateiojekt (Datei, Bibliothek) ausgewählt und von dem Ereignis betroffen ist. Dies ist gleichbedeutend mit einer logischen ODER-Verknüpfung:

**Subjekt ODER Ereignis ODER Dateiojekt**

Die INDEPENDENT Auswahl-Regel bewirkt, dass ein Ereignis protokolliert wird, wenn das Objekt oder Subjekt ausgewählt wurde, auch wenn das Ereignis selbst nicht ausgewählt wurde. Eine Benutzerkennung kann ebenfalls wegen bestimmter ausgewählter Ereignisse oder Objekte protokolliert werden (siehe [Abschnitt „Auswahlverfahren“ auf Seite 24](#)), obwohl sie selbst **nicht** ausgewählt ist.

**PRESELECTION-RULE = \*FILES-BY-EVENTS**

Ist das Subjekt ausgewählt, wird immer protokolliert. Ist das Subjekt nicht ausgewählt, wird nur dann protokolliert, wenn Ereignis und Dateiojekt ausgewählt sind und deren Audit-Attribute mit dem Ereignis-Ergebnis übereinstimmen. Ist das Ereignis kein Dateiojekt-Ereignis, gilt die INDEPENDENT-Regel (siehe [Abschnitt „Auswahlverfahren“ auf Seite 24](#)).

Die Verknüpfungsregel für \*FILES-BY-EVENTS ist folgende:

**Subjekt ODER (Ereignis UND Dateiojekt)****EXIT = \*UNCHANGED / \*YES / \*NO**

Bestimmt, ob der System-Exit Nr.110 (Schreiben der SAT-Daten) aufgerufen werden kann.

**LOGGING-QUANTITY = \*UNCHANGED / \*STD / \*EXTENDED**

Bestimmt, ob \*EXTENDED-Felder in die SATLOG-Datei übernommen werden.

**LOGGING-QUANTITY = \*STD**

\*EXTENDED-Felder werden nicht in die SATLOG-Datei übernommen.

**LOGGING-QUANTITY = \*EXTENDED**

\*EXTENDED-Felder werden in die SATLOG-Datei übernommen.

*Hinweis*

Die Angabe \*EXTENDED ist auch dann notwendig, wenn \*EXTENDED-Felder von einer SAT-Exit-Routine ausgewertet werden sollen.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                                                                                                                                                                   |
|-------|-----|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt<br>Warnung: Unbekanntes Ereignis<br>Warnung: Ereignis nicht umschaltbar<br>Warnung: Benutzerkennung unbekannt<br>Warnung: Benutzerkennung nicht umschaltbar |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                                                                                                                                                                     |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                                                                                                                                                    |
|       | 64  | SAT1020  | Ereignis in Ereignisliste bereits vorhanden                                                                                                                                                 |
|       | 64  | SAT1030  | Benutzer in Benutzerliste bereits vorhanden                                                                                                                                                 |
|       | 64  | SAT1050  | Kommando nur erlaubt, wenn Logging-Funktion aktiviert                                                                                                                                       |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                                                                                                                                                    |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                                                                                                                                                                     |

*Hinweise*

- Die Auswahl-Einstellungen von SAT bei erstem Einsatz bzw. ohne individuelle Steuerung sind:
  - Benutzerkennung: Für bestehende Benutzerkennungen sind die Auswahleinstellungen entsprechend den Einträgen im Benutzerkatalog. Für neu eingerichtete Benutzerkennungen werden alle Ereignisse protokolliert.
  - Ereignis: Voreinstellung sicherheitsrelevanter Ereignisse (siehe „[Tabelle der Objekt Ereignisse](#)“ auf Seite 196)
  - Datei-Objekt: entsprechend den Einträgen im Dateikatalog
  - Verknüpfungsregel: INDEPENDENT-Regel
  - Exit-Aktivierung: System-Exit Nr. 110 nicht aktiv
  - Aufzeichnungsumfang: \*EXTENDED-Felder werden nicht aufgezeichnet
- Ist eine (oder mehrere) der angegebenen Benutzerkennungen im Benutzerkatalog nicht vorhanden, wird eine Fehlermeldung ausgegeben. Für die vorhandenen Benutzerkennungen wird das Kommando ausgeführt. Das gleiche gilt für unbekannte Ereignis-Typen.
- Standardmäßig hat eine mit ADD-USER neu eingerichtete Benutzerkennung AUDIT-SWITCH = ON.  
Werden Benutzerkennungen aus einer Vorgängerversion des BS2000 übernommen, behalten die Benutzerkennungen die bisherigen Einstellungen.
- Gehört ein Ereignis zu einem Produkt, für das die Aktivierung des SAT-Supports mit /MODIFY-SAT-SUPPORT-PARAMETERS gesteuert werden kann (in der aktuellen Version ist dies nur das Produkt POSIX), so wird eine mit /MODIFY-SAT-PRESELECTION

vorgenommene Einstellung für dieses Ereignis immer akzeptiert. Diese Einstellung wird aber bei Auftreten des Ereignisses nur wirksam, wenn für das betreffende Produkt der SAT-Support aktiviert ist.

5. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

### *Beispiele*

1. Der Sicherheitsbeauftragte will:

- in jedem Fall die Ereignis-Typen READ-DATA und DELETE-DATA protokollieren
- RENAME FILE (DVS) in nicht erfolgreichen Fällen protokollieren
- die Benutzerkennungen HUGO und BILL protokollieren
- die Benutzerkennung JAMES nicht protokollieren
- die FILES-BY-EVENTS Auswahl-Regel wählen

Dazu muss er zunächst in der „[Tabelle der Objekteignisse](#)“ auf Seite 196 beim Objekt FILE die Kurznamen für die Operationen 'Datei lesen' (=FRD), 'Datei löschen' (=FDD) und 'Datei umbenennen' (=FRN) herausuchen.

Dann muss er folgendes Kommando eingeben:

```
/modify-sat-preselection -
/   event-auditing=(frd(audit-switch=*on(result=*all)), -
/                       fdd(audit-switch=*on(result=*all)), -
/                       frn(audit-switch=*on(result=*failure))), -
/   user-auditing=(hugo(audit-switch=*on), -
/                   bill(audit-switch=*on), -
/                   james(audit-switch=*off)), -
/   preselection-rule=*files-by-events
```

2. Der Sicherheitsbeauftragte will für jede Benutzerkennung die System-Standard-Protokollierung einschalten, d.h. die Standardeinstellung für die Audit-Attribute der Ereignisse (vgl. „[Tabelle der Objekteignisse](#)“ auf Seite 196). Diese Protokolliereinstellung soll auch für Benutzerkennungen gelten, die erst in Zukunft eingerichtet werden. Hierzu sind zwei Kommandos erforderlich. Mit dem ersten wird die Protokollierung für die bereits bestehenden Benutzerkennungen festgelegt. Das zweite Kommando bezieht sich auf die neu eingerichteten Benutzerkennungen:

```
/modify-sat-preselection -
/   user-auditing=*all-switchable(audit-switch=*off)
/modify-sat-preselection -
/   user-auditing=*default(new-user=*off)
```

## MODIFY-SAT-SUPPORT-PARAMETERS

### Produktspezifische Aktivierung/Deaktivierung von Protokollierung und Alarmen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /MODIFY-SAT-SUPPORT-PARAMETERS kann der Sicherheitbeauftragte die SAT-Protokollierung und die SAT-Alarme produktspezifisch aktivieren oder deaktivieren.

Aktivieren bedeutet, dass für alle Ereignisse des betreffenden Produkts die „normale“ SAT-Protokollierung durchgeführt wird, unter Berücksichtigung der für diese Ereignisse eingestellten Preselection, Filter und Alarme.

Deaktivieren bedeutet, dass für die Ereignisse dieses Produkts generell weder die SAT-Protokollierung noch eine Überprüfung auf Auslösung von Alarmen durchgeführt wird. Dies gilt unabhängig davon, was aufgrund der Preselection für diese Ereignisse eingestellt ist, bzw. welche Alarme definiert sind.

Für ein zu protokollierendes Ereignis wird die mit /MODIFY-SAT-PRESELECTION vorgenommene Einstellung also nur dann wirksam, wenn das Ereignis nicht zu einem Produkt gehört, für das mit /MODIFY-SAT-SUPPORT-PARAMETERS der SAT-Support deaktiviert wurde.

Ebenso wird ein mit /ADD- oder /MODIFY-SAT-ALARM-CONDITION definierter Alarm bei einem bestimmten Ereignis nur ausgelöst, wenn das Ereignis nicht zu einem solchen Produkt gehört.

Derzeit wird die generelle Aktivierung oder Deaktivierung der SAT-Protokollierung nur für das Produkt POSIX unterstützt.

|                                                         |
|---------------------------------------------------------|
| <b>MODIFY-SAT-SUPPORT-PARAMETERS</b>                    |
| <b>POSIX-EVENTS = *UNCHANGED / *DISABLED / *ENABLED</b> |

#### **POSIX-EVENTS =**

Angabe ob für das Produkt POSIX (Portable Open System Interface for UNIX) SAT-Protokollierung und SAT-Alarme aktiviert oder deaktiviert werden.

Betroffene Ereignisse sind die Ereignisse der SAT-Objekte POSIX-FILE-and-Directory, POSIX-PROCESS, POSIX-CHILD-Process und POSIX-SYSTEM-Resources.

**POSIX-EVENTS = \*UNCHANGED**

Die Einstellung für die Ereignisse des angegebenen Produkts bleibt unverändert.

**POSIX-EVENTS = \*DISABLED**

SAT-Protokollierung und -Alarmer werden für das angegebene Produkt deaktiviert. Das bedeutet, dass für die Ereignisse dieses Produkts generell keine SAT-Protokollierung durchgeführt wird und keine SAT-Alarmer ausgelöst werden.

Die Einstellungen der Preselection bzw. die Alarmdefinitionen werden durch die Deaktivierung nicht verändert; sie sind für die betroffenen Ereignisse aber nicht mehr wirksam.

**POSIX-EVENTS = \*ENABLED**

SAT-Protokollierung und -Alarmer werden für das angegebene Produkt aktiviert. Das bedeutet, dass für die Ereignisse dieses Produkts die SAT-Protokollierung entsprechend der Vorgaben durch Preselection und Filter durchgeführt wird, und die Alarmer gemäß Definition ausgelöst werden können.

Die Angabe `POSIX-EVENTS=*ENABLED` **ermöglicht** nur die Protokollierung bzw. Alarmauslösung für die entsprechenden Ereignisse. Die Durchführung der Protokollierung bzw. Alarmierung für diese Ereignisse muss zusätzlich mit dem Kommando `/MODIFY-SAT-PRESELECTION` bzw. `/ADD-SAT-ALARM-CONDITIONS` eingeschaltet werden.

Die Einstellungen der Preselection bzw. die Alarmdefinitionen werden durch die Aktivierung nicht verändert; sie werden für die betroffenen Ereignisse nun wirksam.

*Hinweise*

- Der SAT-Support für POSIX ist standardmäßig ausgeschaltet, und muss explizit eingeschaltet werden, damit die POSIX-Ereignisse protokolliert werden können.
- Änderungen, die der Sicherheitsbeauftragte an den Preselection-Standardvoreinstellungen für POSIX-Ereignisse vornehmen möchte, sind unabhängig von der Einstellung des SAT-Supports und können jederzeit durchgeführt und sichergestellt werden.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                                                  |
|-------|-----|----------|----------------------------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                                            |
|       | 32  | SAT0000  | Nicht behebbarer Fehler.<br>SATCP ist evtl. in einem inkonsistenten Status |
|       | 32  | SAT5000  | Nicht behebbarer Fehler                                                    |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                                   |
|       | 64  | SAT1050  | Kommando nur erlaubt, wenn Logging-Funktion aktiviert                      |
|       | 130 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                                   |
|       | 130 | SAT1080  | Wechsel in Vorbereitung                                                    |

*Beispiel*

Der Sicherheitsbeauftragte schaltet den SAT-Support für die POSIX-Ereignisse ein:

```
/modify-sat-support-parameters posix-events=*enabled
```

## REMOVE-SAT-ALARM-CONDITIONS

### Alarmdefinition entfernen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /REMOVE-SAT-ALARM-CONDITIONS kann eine bestehende Alarmdefinition entfernt werden.

**REMOVE-SAT-ALARM-CONDITIONS**

**NAME** = \*ALL / list-poss(32): <name 1..8>

**NAME = list-poss(32):<name 1..8> / \*ALL**

Name des zu entfernenden Alarms. Dieser Name wurde mit /ADD-SAT-ALARM-CONDITIONS definiert.

**NAME = \*ALL**

Alle Alarmdefinitionen werden entfernt.

#### Kommando-Returncode

| (SC2) | SC1 | Maincode | Bedeutung                                             |
|-------|-----|----------|-------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                       |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                               |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert              |
|       | 64  | SAT1021  | Alarm in Alarmliste bereits vorhanden                 |
|       | 64  | SAT1028  | Alarm unbekannt                                       |
|       | 64  | SAT1050  | Kommando nur erlaubt, wenn Logging-Funktion aktiviert |
|       | 64  | SAT1070  | Alarmtabelle ist leer                                 |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt              |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                               |

#### Hinweise

Siehe allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

## REMOVE-SAT-FILTER-CONDITIONS

### Filterdefinition entfernen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /REMOVE-SAT-FILTER-CONDITIONS kann eine bestehende Filterdefinition entfernt werden.

**REMOVE-SAT-FILTER-CONDITIONS**

**NAME** = \*ALL / list-poss(32): <name 1..8>

**NAME = list-poss(32):<name 1..8> / \*ALL**

Name des zu entfernenden Filters. Dieser Name wurde mit /ADD-SAT-FILTER-CONDITIONS definiert.

**NAME = \*ALL**

Alle Filterdefinitionen werden entfernt.

### Kommando-Returncode

| (SC2) | SC1 | Maincode | Bedeutung                                             |
|-------|-----|----------|-------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                       |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                               |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert              |
|       | 64  | SAT1031  | Filter in Filterliste bereits vorhanden               |
|       | 64  | SAT1032  | Filter unbekannt                                      |
|       | 64  | SAT1050  | Kommando nur erlaubt, wenn Logging-Funktion aktiviert |
|       | 64  | SAT1072  | Filtertabelle ist leer                                |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt              |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                               |

### Hinweise

Siehe allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

## RESUME-SAT-LOGGING

### Protokollierung fortsetzen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /RESUME-SAT-LOGGING reaktiviert der Sicherheitsbeauftragte (Kennung mit dem Privileg SECURITY-ADMINISTRATION) die Protokollierung von Ereignissen sowie die Überwachung durch die SAT-Alarm-Funktion, die er beide zuvor mit /HOLD-SAT-LOGGING aufgehoben hatte. Zugleich eröffnet er damit eine neue SATLOG-Datei.

|                    |
|--------------------|
| RESUME-SAT-LOGGING |
|                    |

Dieses Kommando hat keine Operanden.

#### Kommando-Returncode

| (SC2) | SC1 | Maincode | Bedeutung                                                              |
|-------|-----|----------|------------------------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                                        |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                                                |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                               |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                               |
|       | 128 | SAT1011  | Verarbeitung eines HOLD-SAT-LOGGING-Kommandos noch nicht abgeschlossen |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                                                |
|       | 128 | SAT2000  | Logging-Funktion bereits aktiviert                                     |
| 2     | 128 | SAT2030  | DVS-Fehler beim Eröffnen der Datei                                     |

*Hinweise*

1. Das Kommando wird zurückgewiesen, wenn SATCP nicht im HOLD-Zustand ist.
2. Die Protokollier-Einstellung bei Ausführung des Kommandos RESUME-SAT-LOGGING ist dieselbe, die vor dem Anhalten von SATCP gültig war.
3. Nach erfolgreicher Ausführung des Kommandos ist SATCP für die Protokollierung bereit und schreibt in die neu eröffnete SATLOG-Datei.
4. Die neue SATLOG-Datei wird auf dem Standard-Pubset der Benutzerkennung SYSAUDIT katalogisiert. Sie wird auf dem Datenträger angelegt, der beim zuletzt angegebenen Kommando /CHANGE-SAT-FILE eingestellt war. Tritt während des Erstellens der SATLOG-Datei ein DVS-Fehler auf (z.B. wenn das Standard-Pubset nicht zur Verfügung steht), dann wird die SATLOG-Datei auf dem Home-Pubset erstellt.
5. Das Kommando RESUME-SAT-LOGGING sollte wegen der Serialisierung und der entstehenden Sicherheitslücken nicht dazu verwendet werden, die SATLOG-Datei zu wechseln. Für diese Aufgabe steht das Kommando /CHANGE-SAT-FILE zur Verfügung.
6. Wenn das Kommando /RESUME-SAT-LOGGING unmittelbar nach dem Kommando /HOLD-SAT-LOGGING eingegeben wird, wird unter Umständen ein Fehler angezeigt. Die Verarbeitung des Kommandos /HOLD-SAT-LOGGING benötigt eine gewisse Zeit, um die SAT-Umgebung asynchron in den Status HOLD zu versetzen. Erst wenn dieser Zustand erreicht ist, ist ein Fortsetzen möglich.
7. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

## SAVE-SAT-PARAMETERS SATCP-Einstellungen speichern

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION, SAT-FILE-MANAGEMENT

Das Kommando /SAVE-SAT-PARAMETERS erlaubt dem Sicherheitsbeauftragten oder SAT-Datei-Verwalter, EVENT-PRESELECTION, Alarm- und Filterdefinitionen, Einstellungen der SAT-Support-Parameter und SATLOG-Datei-Attribute für die nächste Sitzung zu speichern. Fehlende oder fehlerhafte Werte werden von SAT mit den Standard-Werten ergänzt.

Die SAT-Parameter-Datei wird immer auf dem Home-Pubset mit dem Namen \$SYSAUDIT.SYSPAR.SAT angelegt.

Die Standard-Werte lauten wie folgt:

EVENT-PRESELECTION: – Ereignis: Voreinstellung sicherheitsrelevanter Ereignisse (siehe „[Tabelle der Objekteignisse](#)“ auf Seite 196)  
– Benutzerkennungen: Für neu eingerichtete Benutzerkennungen werden alle Ereignisse protokolliert.  
– Verknüpfungsregel: INDEPENDENT-Regel  
– Exit-Aktivierung: System-Exit Nr. 110 nicht aktiv  
– Aufzeichnungsumfang: \*EXTENDED-Felder werden nicht protokolliert

FILTER-CONDITIONS: kein Filter definiert

ALARM-CONDITIONS: kein Alarm definiert

SAT-FILE-ATTRIBUTES: BUFFER-LENGTH=\*STD(SIZE=2),  
SPACE=\*RELATIVE(PRIMARY-ALLOCATION=120,  
SECONDARY-ALLOCATION=120)

SAT-SUPPORT POSIX-EVENTS=\*DISABLED

**SAVE-SAT-PARAMETERS**

**EVENT-PRESELECTION** = \*UNCHANGED / \*STD / \*CURRENT

,**ALARM-CONDITIONS** = \*UNCHANGED / \*STD / \*CURRENT

,**SAT-FILE-ATTRIBUTES** = \*UNCHANGED / \*STD / \*CURRENT

,**FILTER-CONDITIONS** = \*UNCHANGED / \*STD / \*CURRENT

,**SAT-SUPPORT** = \*UNCHANGED / \*STD / \*CURRENT

**EVENT-PRESELECTION =**

Dieser Operand steht nur dem Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) zur Verfügung.

**EVENT-PRESELECTION = \*UNCHANGED**

Die SAT-Parameter-Datei wird für EVENT-PRESELECTION nicht geändert.

**EVENT-PRESELECTION = \*STD**

In der SAT-Parameter-Datei werden für EVENT-PRESELECTION die Standard-Werte eingetragen. Die Standard-Werte entnehmen Sie der Tabelle „Objekt-Ereignisse, Kurznamen und Audit-Attribute“ auf Seite 197ff.

**EVENT-PRESELECTION = \*CURRENT**

Es werden die momentan gültigen Werte in die SAT-Parameter-Datei eingetragen, die mit /SHOW-SAT-STATUS angezeigt werden können.

**ALARM-CONDITIONS =**

Dieser Operand steht nur dem Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) zur Verfügung.

**ALARM-CONDITIONS = \*UNCHANGED**

Die SAT-Parameter-Datei wird für ALARM-CONDITIONS nicht geändert.

**ALARM-CONDITIONS = \*STD**

In der SAT-Parameter-Datei werden für ALARM-CONDITIONS die Standard-Werte eingetragen. Dies bedeutet, dass es **keine** Alarmdefinitionen gibt.

**ALARM-CONDITIONS = \*CURRENT**

Es werden die momentan gültigen Werte in die SAT-Parameter-Datei eingetragen, die mit SHOW-SAT-ALARM-CONDITIONS angezeigt werden können.

**SAT-FILE-ATTRIBUTES =**

Dieser Operand steht nur dem SAT-Datei-Verwalter (Privileg SAT-FILE-MANAGEMENT) zur Verfügung.

**SAT-FILE-ATTRIBUTES = \*UNCHANGED**

Die SAT-Parameter-Datei wird für SAT-FILE-ATTRIBUTES nicht geändert.

**SAT-FILE-ATTRIBUTES = \*STD**

In der SAT-Parameter-Datei werden für SAT-FILE-ATTRIBUTES die Standard-Werte eingetragen (siehe Anfang dieses Abschnitts).

**SAT-FILE-ATTRIBUTES = \*CURRENT**

Es werden die momentan gültigen Attribute in die SAT-Parameter-Datei eingetragen.

**FILTER-CONDITIONS =**

Dieser Operand steht nur dem Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) zur Verfügung.

**FILTER-CONDITIONS = \*UNCHANGED**

Die SAT-Parameter-Datei wird für FILTER-CONDITIONS nicht geändert.

**FILTER-CONDITIONS = \*STD**

In der SAT-Parameter-Datei werden für FILTER-CONDITIONS die Standard-Werte eingetragen. Dies bedeutet, dass es **keine** Filterdefinitionen gibt.

**FILTER-CONDITIONS = \*CURRENT**

Es werden die momentan gültigen Werte in die SAT-Parameter-Datei eingetragen, die mit /SHOW-SAT-FILTER-CONDITIONS angezeigt werden können.

**SAT-SUPPORT =**

Dieser Operand steht nur dem Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) zur Verfügung.

**SAT-SUPPORT = \*UNCHANGED**

Die SAT-Parameter-Datei wird für SAT-SUPPORT nicht geändert.

**SAT-SUPPORT = \*STD**

In der SAT-Parameter-Datei werden für SAT-SUPPORT die Standard-Werte eingetragen (siehe am Anfang dieser Kommandobeschreibung auf [Seite 120](#)).

**SAT-SUPPORT = \*CURRENT**

Es werden die momentan gültigen Werte in die SAT-Parameter-Datei eingetragen, die mit /SHOW-SAT-SUPPORT-PARAMETERS angezeigt werden können.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                                                                                                                                                                                 |
|-------|-----|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt<br>SAT-Parameterdatei geöffnet<br>Warnung: Prüffehler                                                                                                                     |
|       | 32  | CMD0221  | Nicht behebbarer Fehler<br>DVS-Fehler<br>SAT-Parameterdatei nicht gültig<br>Abnormale Beendigung von SATCP<br>Fehler während Initialisierung von SATCP<br>Fehler während Initialisierung von SAVE/RESTORE |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                                                                                                                                                                  |
|       | 64  | SAT1050  | Kommando nur erlaubt, wenn Logging-Funktion aktiviert                                                                                                                                                     |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                                                                                                                                                                  |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                                                                                                                                                                                   |

*Hinweise*

1. Bei Angabe der Werte \*STD oder \*CURRENT für einen oder mehrere Parameter, werden die Werte überschrieben, die vorher hinterlegt waren.
2. Siehe auch allgemeine Hinweise zur SAT-Parameterdatei auf [Seite 41](#).
3. Siehe auch allgemeine Hinweise zu den SAT-Kommandos auf [Seite 59](#).

## SHOW-SAT-ALARM-CONDITIONS SAT-Alarmdefinitionen anzeigen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Das Kommando /SHOW-SAT-ALARM-CONDITIONS zeigt Informationen über Alarmdefinitionen an.

### SHOW-SAT-ALARM-CONDITIONS

```

NAME = *ALL / list-poss(32): <name 1..8>
,INFORMATION = *ALL / *NAME
,VALUE = *CURRENT / *STD / *NEXT-SESSION
,OUTPUT = *SYSOUT / *SYSLST(...)
    *SYSLST(...)
        | LINES-PER-PAGE = 64 / <integer 20..255>
  
```

**NAME = \*ALL / list-poss(32): <name 1..8>**  
Bestimmt den Informationsumfang der Anzeige.

#### **INFORMATION =**

Legt fest, welche Information zu einer Alarmdefinition ausgegeben werden soll.

#### **INFORMATION = \*ALL**

Es werden alle Informationen (Name, Definitionen und Reaktion) angezeigt.

#### **INFORMATION = \*NAME**

Es wird nur der Name der Definition angezeigt.

#### **VALUE =**

Auswahl der auszugebenden Alarmdefinitionen. Je nach dem, ob die aktuellen Alarmdefinitionen bereits in der SAT-Parameter-Datei gespeichert wurden oder nicht, ergeben sich Unterschiede im Umfang der Ausgabe.

**VALUE = \*CURRENT**

Es werden die aktuellen Alarmdefinitionen angezeigt. Wurden seit dem Start von SATCP Änderungen an den Alarmdefinitionen vorgenommen, ohne dass diese in der SAT-Parameter-Datei gespeichert wurden, unterscheiden sich die Definitionen der momentanen Sitzung und der folgenden, da SATCP beim nächsten Start die Definitionen der SAT-Parameter-Datei liest.

**VALUE = \*STD**

Der Standardwert für Alarmdefinitionen wird ausgegeben. Derzeit existieren standardmäßig keine Alarmdefinitionen.

**VALUE = \*NEXT-SESSION**

Diese Funktion zeigt den Inhalt der SAT-Parameter-Datei an. Wurden seit dem Start von SATCP Änderungen an den Alarmdefinitionen vorgenommen, ohne dass diese in der SAT-Parameter-Datei gespeichert wurden, unterscheiden sich die Definitionen der momentanen Sitzung und der folgenden, da SATCP beim nächsten Start die Definitionen der SAT-Parameter-Datei liest.

**OUTPUT = \*SYSOUT**

Die angeforderte Information wird auf SYSOUT ausgegeben.

**OUTPUT = \*SYSLST(...)**

Die angeforderte Information wird auf SYSLST ausgegeben.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                          |
|-------|-----|----------|----------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                    |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                            |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert           |
|       | 64  | SAT1021  | Alarm in Alarmliste bereits vorhanden              |
|       | 64  | SAT1028  | Alarm unbekannt                                    |
|       | 64  | SAT1070  | Aktuell ist kein Alarm definiert                   |
|       | 64  | SAT1074  | Standardmäßig ist kein Alarm definiert             |
|       | 64  | SAT1075  | In der SAT-Parameterdatei ist kein Alarm definiert |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt           |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                            |
|       | 128 | SAT4010  | SAT-Parameterdatei derzeit nicht verfügbar         |

*Hinweise*

- Das Kommando schreibt nicht in S-Variable, weil es nur vom Sicherheitsbeauftragten ausgeführt werden darf. Dieser hat jedoch nicht das Privileg STD-PROCESSING, das für die Bearbeitung von S-Variablen erforderlich ist.
- Die Ausgabe der Felder filpos, curlim2 und maxlim2 erfolgt immer in Vielfachen von 512 Byte zusammen mit Maßeinheit „(512 B)“.

*Beispiel*

Folgende Alarmbedingungen seien definiert:

```
/add-sat-alarm-conditions alarm1, -
/      select=*par ( -
/      field-name=( -
/      *filpos(value=( -
/          512(unit=*kb),10240(unit=*bytes),6(unit=*mb))), -
/      *curlim(value=(513,10240,7)), -
/      *curlim2(value=( -
/          1024(unit=*kb),1536(unit=*bytes),2(unit=*mb))))
```

Diese Alarmbedingungen werden folgendermaßen ausgegeben:

```
/show-sat-alarm-conditions alarm1
ALARM NAME = ALARM1      TIME-LIMIT = UNDEFINED      REPEAT = 3
      TRIGGER-ACTION = OPERATOR-MESSAGE (WAIT-RESPONSE = YES)
EVENTS : *ALL
USERS  : *ALL
FIELD  : CURLIM
      ONLY VALUES : 7 / 513 / 10240
FIELD  : FILPOS
      ONLY VALUES : 20 (512B) / 1024 (512B) / 12288 (512B)
FIELD  : CURLIM2
      ONLY VALUES : 3 (512B) / 2048 (512B) / 4096 (512B)
```

- Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

Der Sicherheitsbeauftragte möchte eine Liste mit bereits eingetragenen Alarmdefinitionen ausgeben, die er im nächsten Lauf verwenden will.

```
/show-sat-alarm-conditions information=*name,value=*next-session
```

## SHOW-SAT-FILTER-CONDITIONS

### SAT-Filterdefinitionen anzeigen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Das Kommando /SHOW-SAT-FILTER-CONDITIONS zeigt Informationen über Filterdefinitionen an.

#### SHOW-SAT-FILTER-CONDITIONS

```

NAME = *ALL / list-poss(32): <name 1..8>
, INFORMATION = *ALL / *NAME
, VALUE = *CURRENT / *STD / *NEXT-SESSION
, OUTPUT = *SYSOUT / *SYSLST(...)
  *SYSLST(...)
    | LINES-PER-PAGE = 64 / <integer 20..255>

```

**NAME = \*ALL / list-poss(32): <name 1..8>**  
Bestimmt den Informationsumfang der Anzeige.

#### **INFORMATION =**

Legt fest, welche Information zu einer Filterdefinition ausgegeben werden soll.

#### **INFORMATION = \*ALL**

Es werden alle Informationen (Name, Definitionen und Reaktion) angezeigt.

#### **INFORMATION = \*NAME**

Es wird nur der Name der Definition angezeigt.

#### **VALUE =**

Auswahl der auszugebenden Filterdefinitionen. Je nach dem, ob die aktuellen Filterdefinitionen bereits in der SAT-Parameter-Datei gespeichert wurden oder nicht, ergeben sich Unterschiede im Umfang der Ausgabe.

**VALUE = \*CURRENT**

Es werden die aktuellen Filterdefinitionen angezeigt. Wurden seit dem Start von SATCP Änderungen an den Filterdefinitionen vorgenommen, ohne dass diese in der SAT-Parameter-Datei gespeichert wurden, unterscheiden sich die Definitionen der momentanen Sitzung und der folgenden, da SATCP beim nächsten Start die Definitionen der SAT-Parameter-Datei liest.

**VALUE = \*STD**

Der Standardwert für Filterdefinitionen wird ausgegeben. Derzeit existieren standardmäßig keine Filterdefinitionen.

**VALUE = \*NEXT-SESSION**

Diese Funktion zeigt den Inhalt der SAT-Parameter-Datei an. Wurden seit dem Start von SATCP Änderungen an den Filterdefinitionen vorgenommen, ohne dass diese in der SAT-Parameter-Datei gespeichert wurden, unterscheiden sich die Definitionen der momentanen Sitzung und der folgenden, da SATCP beim nächsten Start die Definitionen der SAT-Parameter-Datei liest.

**OUTPUT = \*SYSOUT**

Die angeforderte Information wird auf SYSOUT ausgegeben.

**OUTPUT = \*SYSLST(...)**

Die angeforderte Information wird auf SYSLST ausgegeben.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                           |
|-------|-----|----------|-----------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                     |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                             |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert            |
|       | 64  | SAT1031  | Filter in Filterliste bereits vorhanden             |
|       | 64  | SAT1032  | Filter unbekannt                                    |
|       | 64  | SAT1072  | Aktuell ist kein Filter definiert                   |
|       | 64  | SAT1076  | Standardmäßig ist kein Filter definiert             |
|       | 64  | SAT1077  | In der SAT-Parameterdatei ist kein Filter definiert |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit. ausgeführt           |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                             |
|       | 128 | SAT4010  | SAT-Parameterdatei derzeit nicht verfügbar          |

*Hinweise*

- Dieses Kommando schreibt keine S-Variablen. Das Kommando darf nur in einer Kennung mit dem Privileg SECURITY-ADMINISTRATION aufgerufen werden. Eine solche Kennung hat jedoch nicht das für SDF-P erforderliche Privileg STD-PROCESSING.

- Die Ausgabe der Felder filpos, curlim2 und maxlim2 erfolgt immer in Vielfachen von 512 Byte zusammen mit Maßeinheit „(512 B)“.

*Beispiel*

Folgende Filterbedingungen seien definiert:

```
/add-sat-filter-conditions filter1, -
/   select=*par ( -
/     field-name=( -
/       *filpos(value=( -
/         512(unit=*kb),10240(unit=*bytes),6(unit=*mb))), -
/       *curlim(value=(513,10240,7)), -
/       *curlim2(value=( -
/         1024(unit=*kb),1536(unit=*bytes),2(unit=*mb))))
```

Diese Alarmbedingungen werden folgendermaßen ausgegeben:

```
/show-sat-filter-conditions filter1
FILTER NAME = FILTER1
TRIGGER-ACTION = LOGGING (RECORDING = YES)
EVENTS : *ALL
USERS : *ALL
FIELD : CURLIM
        ONLY VALUES : 7 / 513 / 10240
FIELD : FILPOS
        ONLY VALUES : 20 (512B) / 1024 (512B) / 12288 (512B)
FIELD : CURLIM2
        ONLY VALUES : 3 (512B) / 2048 (512B) / 4096 (512B)
```

- Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiel*

Der Sicherheitsbeauftragte möchte eine Liste mit bereits eingetragenen Filterdefinitionen ausgeben, die er im nächsten Lauf verwenden will.

```
/show-sat-filter-conditions information=*name,value=*next-session
```

## SHOW-SAT-STATUS

### SAT-Zustand anzeigen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION, SAT-FILE-MANAGEMENT

Mit dem Kommando /SHOW-SAT-STATUS kann der Sicherheitsbeauftragte und der SAT-Datei-Verwalter Informationen über die SAT-Protokollierung ausgeben lassen.

#### SHOW-SAT-STATUS

```

INFORMATION = *SUMMARY / list-poss(5): *LOGGING-STATUS / *COLLECTION-FILE /
*PRESELECTION-RULE / *EVENT-AUDITING(...) / *USER-AUDITING(...)

*EVENT-AUDITING(...)
  |
  | EVENT-NAME = *ALL(...) / list-poss(50): <name 3..3>
  |
  | *ALL(...)
  | |
  | | AUDIT-SWITCH = *IGNORE / *ON(...) / *OFF
  | |
  | | *ON(...)
  | | |
  | | | RESULT = *ALL / *SUCCESS / *FAILURE
  |
  | *USER-AUDITING(...)
  | |
  | | USER-IDENTIFICATION = *ALL-SWITCHABLE(...) / *ALL(...) / list-poss(50): <name 1..8>
  | |
  | | *ALL-SWITCHABLE(...)
  | | |
  | | | AUDIT-SWITCH = *IGNORE / *ON / *OFF
  | |
  | | *ALL(...)
  | | |
  | | | AUDIT-SWITCH = *IGNORE / *ON / *OFF
  |
  | ,OUTPUT = *SYSOUT / *SYSLST(...)
  |
  | *SYSLST(...)
  | |
  | | LINES-PER-PAGE = 64 / <integer 20..255>
  |
  | ,VALUE = *CURRENT / *STD / *NEXT-SESSION

```

**INFORMATION =**

Bestimmt, welche Informationen ausgegeben werden.

**INFORMATION = \*SUMMARY**

Gibt die unter LOGGING-STATUS, COLLECTION-FILE und PRESELECTION-RULE beschriebenen Informationen aus. Aus Kompatibilitätsgründen wird der Wert \*STD an Stelle von \*SUMMARY noch unterstützt.

**INFORMATION = \*LOGGING-STATUS**

Gibt den aktuellen Zustand der SAT-Protokollierung aus (RECORD, HOLD, NO RESOURCE, SHUTDOWN).

**INFORMATION = \*COLLECTION-FILE**

Gibt die Merkmale der aktuellen SATLOG-Datei aus (Name, SUPPORT, BUFFER-LENGTH, PRIMARY-ALLOCATION und SECONDARY-ALLOCATION).

**INFORMATION = \*PRESELECTION-RULE**

Zeigt folgende Informationen an:

- die aktuelle Auswahl-Regel : \*INDEPENDENT oder \*FILES-BY-EVENTS
- den Aufzeichnungsumfang: \*STD oder \*EXTENDED
- die EXIT-Aktivierung: \*YES oder \*NO
- den Standardwert für die Protokolliereinstellung neu eingerichteter Benutzerkennungen: \*ON oder \*OFF.

**INFORMATION = \*EVENT-AUDITING(...)**

Gibt Informationen über Ereignisse aus.

**EVENT-NAME = \*ALL(...)**

Zeigt die Ereignisse, die eine bestimmte Protokollier-Einstellung haben.

**AUDIT-SWITCH = \*IGNORE**

Gibt eine Liste aller Ereignisse aus, unabhängig von ihrer Protokollier-Einstellung.

**AUDIT-SWITCH = \*ON**

Gibt die Liste aller Ereignisse aus, deren Protokollierung eingeschaltet ist.

**RESULT = \*ALL / \*SUCCESS / \*FAILURE**

Gibt die Liste aller Ereignisse aus, deren Protokollierung eingeschaltet ist und deren Audit-Attribute den mit RESULT angegebenen Wert haben.

**AUDIT-SWITCH = \*OFF**

Gibt die Liste aller Ereignisse aus, deren Protokollierung ausgeschaltet ist.

**EVENT-NAME = <name 3..3>**

Zeigt die Protokollier-Einstellung der angegebenen Ereignisse. Die Eingabe besteht aus dem 3-stelligen Kurznamen der Ereignis-Typen, z.B. FCD, FRD,... (siehe „[Tabelle der Objekteignisse](#)“ auf Seite 196).

**INFORMATION = \*USER-AUDITING(...)**

Zeigt, welche Benutzer für die Protokollierung ausgewählt sind.

**USER-IDENTIFICATION = \*ALL-SWITCHABLE(...)**

Zeigt die schaltbaren Benutzerkennungen, die ein bestimmtes Audit-Attribut haben (Kennung des Sicherheitsbeauftragten, SYSAUDIT und solche mit dem Privileg SAT-Datei-Verwaltung sind keine schaltbaren Benutzerkennungen).

**AUDIT-SWITCH = \*IGNORE / \*ON / \*OFF**

Das Audit-Attribut für die schaltbaren Benutzerkennungen soll entweder ein- oder ausgeschaltet sein oder im Standardfall ignoriert werden.

**USER-IDENTIFICATION = \*ALL(...)**

Zeigt alle Benutzerkennungen, die ein bestimmtes Audit-Attribut haben.

**AUDIT-SWITCH = \*IGNORE / \*ON / \*OFF**

Das Audit-Attribut für die Benutzerkennungen soll entweder ein- oder ausgeschaltet sein oder im Standardfall ignoriert werden.

**USER-IDENTIFICATION = <name 1..8>**

Die Protokollier-Einstellung der angegebenen Benutzerkennung wird angezeigt.

**OUTPUT = \*SYSOUT**

Die angeforderte Information wird auf SYSOUT ausgegeben.

**OUTPUT = \*SYSLST(...)**

Die angeforderte Information wird auf SYSLST ausgegeben.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

**VALUE = \*CURRENT / \*STD / \*NEXT-SESSION**

Gibt an, welche Informationen ausgegeben werden sollen:

Die momentan gültigen, die Standard-Werte oder die in der nächsten Sitzung gültigen.

Die Liste der Benutzerkennungen wird nur ausgegeben wenn INFORMATION=USER-AUDITING und VALUE=CURRENT.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                                |
|-------|-----|----------|----------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                          |
|       | 32  | SAT0000  | Nicht behebbarer Fehler                                  |
|       | 32  | CMD2009  | Systemfehler bei Ausgabe der S-Variablen                 |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                 |
|       | 64  | SAT1020  | Ereignis in Ereignisliste bereits vorhanden              |
|       | 64  | SAT1030  | Benutzer in Benutzerliste bereits vorhanden              |
|       | 64  | SAT1040  | Information in Informationsliste bereits vorhanden       |
|       | 64  | SAT1060  | Keine Information vorhanden                              |
|       | 64  | OPS0002  | Ausgabe der S-Variablen wurde unterbrochen               |
|       | 128 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                 |
|       | 128 | SAT1080  | Wechsel in Vorbereitung                                  |
|       | 128 | SAT4010  | SAT-Parameterdatei derzeit nicht verfügbar               |
|       | 130 | OPS0001  | Ausgabe der S-Variablen konnte nicht durchgeführt werden |

*Hinweise*

1. Ist eine (oder sind mehrere) der angegebenen Benutzerkennung(en) im Benutzerkatalog nicht vorhanden, wird eine Meldung ausgegeben. Das Kommando wird dennoch für die vorhandenen Benutzerkennungen ausgeführt. Das gleiche gilt für unbekannte Ereignisse.
2. Das Kommando wird abgewiesen, wenn in der Liste der Ereignisse oder in der Liste der Benutzerkennungen gleiche Ereignisse oder Benutzerkennungen mehrfach auftreten.
3. Die Protokollier-Einstellung der Ereignisse und Benutzerkennungen wird bei der Ausgabe mit einem Stern (\*) versehen, wenn diese Protokollier-Einstellung nicht verändert werden kann.

Beispiel: **USER-AUDITING**

```
SYSAUDIT *ON  SYSPRIV *ON  TSOS OFF
```

4. Siehe auch allgemeine Hinweise zu den SAT-Kommandos [auf Seite 59](#).

*Beispiele*

1. Der Sicherheitsbeauftragte möchte über den aktuellen Status von SAT, über die zugewiesene SATLOG-Datei und die gültige Verknüpfungsregel informiert werden:

```
/show-sat-status
```

Er erhält folgende Ausgabe

```
SAT SUBSYSTEM VERSION 05.5A00                               VALUE = CURRENT
LOGGING-STATUS      : RECORD
COLLECTION-FILE(SATLOG) :
FILENAME   : :A:$SYSAUDIT.SYS.SATLOG.2017-05-02.003.01
STATUS    : OPENED - VSN :          - DEVICE :
BLOCK     : (STD,2)
SPACE     : (120,120)
REPEAT    : NO
PRESELECTION-RULE : INDEPENDENT
BY-EXIT   : NO
LOGGING-QUANTITY  : STD
USER-AUDITING DEFAULT : ON
```

2. Der Sicherheitsbeauftragte will ausschließlich die Ereignisse ausgeben, die für die Protokollierung ausgewählt sind (RESULT = ALL):

```
/show-sat-status information= -
/      *event-auditing(event-name=*all(audit-switch=*on(result=*all)))
```

oder in Kurzform:

```
/show-sat-stat inf=*event-audit(event-name=*all(audit-switch=*on))
```

3. Der Sicherheitsbeauftragte will

- die Protokollier-Einstellung aller Ereignisse anzeigen
- Informationen über die Protokollier-Einstellung der Benutzerkennungen BILL, HUGO und JAMES:

```
/show-sat-status information=( -
/      *event-auditing(event-name=*all), -
/      *user-auditing(user-identification=(bill,hugo,james)))
```

oder in Kurzform:

```
/show-sat-stat (event-audit,user-audit((bill,hugo,james)))
```

## Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

| Schreibweise im Kommando        | gekürzte Schreibweise in Tabelle |
|---------------------------------|----------------------------------|
| INFORMATION = SUMMARY           | 1                                |
| INFORMATION = LOGGING-STATUS    | 2                                |
| INFORMATION = COLLECTION-FILE   | 3                                |
| INFORMATION = PRESELECTION-RULE | 4                                |
| INFORMATION = EVENT-AUTDITING   | 5                                |
| INFORMATION = USER-AUDITING     | 6                                |

Zusätzliche Bedingungen, die mit den Angaben von INFORMATION zusammenwirken:

| Zusätzlich Bedingungen                       | gekürzte Schreibweise in Tabelle |
|----------------------------------------------|----------------------------------|
| Wertzuweisung, nur wenn LOG-F.SUP-TYPE=*PRIV | a                                |
| Wertzuweisung, nur wenn LOG-F.REPEAT=*TRUE   | b                                |

Die nachfolgende Tabelle ist nach dem Namen der S-Variablen sortiert. Die Spalte T (Typ) bezeichnet den Datentyp des Inhalts: S (string), I (integer), B (boolean).

| Ausgabe-Information                                                                                                   | Name der S-Variablen                       | T | Inhalt                                  | Bedingung |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------|---|-----------------------------------------|-----------|
| Audit-Attribut des Ereignisses in SATLOG-Datei, das bestimmt, ob ein Ereignis für die Protokollierung ausgewählt wird | var(*LIST).EVENT-AUDIT(*LIST).AUDIT-SWITCH | S | *OFF<br>*ON-ALL<br>*ON-FAIL<br>*ON-SUCC | 5         |
| Kurzname des Ereignistyps, dessen Protokollier-Einstellung angezeigt wird                                             | var(*LIST).EVENT-AUDIT(*LIST).EVENT-NAME   | S | <name 3..3>                             | 5         |
| Ereignis wurde für Protokollierung ausgewählt                                                                         | var(*LIST).EVENT-AUDIT(*LIST).SWITCHABLE   | B | FALSE<br>TRUE                           | 5         |
| Puffergröße der SATLOG-Datei                                                                                          | var(*LIST).LOG-F.BUF-LEN                   | I | <integer 1..16><br><buffer-length>      | 1,3       |
| Gerätetyp des Plattenspeichers, auf dem die SATLOG-Datei gespeichert ist                                              | var(*LIST).LOG-F.DEV-TYPE                  | S | <dev-type>                              | a         |
| Name der SATLOG-Datei                                                                                                 | var(*LIST).LOG-F.NAME                      | S | <filename>                              | 1,3       |
| SATLOG-Datei ist geöffnet                                                                                             | var(*LIST).LOG-F.OPEN                      | B | FALSE<br>TRUE                           | 1,3       |
| Zeitintervall (in Tagen), nach dessen Ablauf der automatische Wechsel der SATLOG-Datei erfolgt                        | var(*LIST).LOG-F.PERIOD-DAYS               | I | <integer 0..10>                         | b         |

(Teil 1 von 2)

| Ausgabe-Information                                                                                   | Name der S-Variablen                          | T | Inhalt                           | Bedingung |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------|---|----------------------------------|-----------|
| Zeitintervall (in Stunden), nach dessen Ablauf der automatische Wechsel der SATLOG-Datei erfolgt      | var(*LIST).LOG-F.PERIOD-HOURS                 | I | <integer 0..23>                  | b         |
| primäre Speicherplatzzuweisung für SATLOG-Datei                                                       | var(*LIST).LOG-F.PRIMARY-ALLOC                | I | <integer>                        | 1,3       |
| die SATLOG-Datei wird automatisch gewechselt                                                          | var(*LIST).LOG-F.REPEAT                       | B | FALSE<br>TRUE                    | 1,3       |
| sekundäre Speicherplatzzuweisung für SATLOG-Datei                                                     | var(*LIST).LOG-F.SECONDARY-ALLOC              | I | <integer 0..32767>               | 1,3       |
| Plattenspeichertyp, auf dem die SATLOG-Datei gespeichert ist                                          | var(*LIST).LOG-F.SUP-TYPE                     | S | *PRIV<br>*PUBLIC                 | 1,3       |
| Archivnummer des Plattenspeichers, auf dem die SATLOG-Datei gespeichert ist                           | var(*LIST).LOG-F.VOL                          | S | <vsn 1..6>                       | a         |
| aktueller SAT-Zustand                                                                                 | var(*LIST).LOG-STA                            | S | *HOLD<br>*NO-RESOURCE<br>*REC    | 1,2       |
| die EXIT-Routine Nr. 110 kann aufgerufen werden                                                       | var(*LIST).PRESEL-RULE.EXIT                   | S | *NO<br>*YES                      | 1,4       |
| Aufzeichnungsumfang                                                                                   | var(*LIST).PRESEL-RULE.QUANTITY               | S | *STD<br>*EXTENDED                | 1,4       |
| Art der Verknüpfungsregel für die Protokollierung des Ereignisses                                     | var(*LIST).PRESEL-RULE.RULE                   | S | *FILES-BY-EVENTS<br>*INDEPENDENT | 1,4       |
| Defaultwert für die die Protokollierung neu eingerichteter Benutzerkennungen                          | var(*LIST).PRESEL-RULE.USER-AUDIT-DEF         | S | *OFF<br>*ON                      | 1,4       |
| Audit-Attribut des Subjekts, das bestimmt, ob die Ereignisse der Benutzerkennung protokolliert werden | var(*LIST).USER-AUDIT(*LIST).<br>AUDIT-SWITCH | S | *OFF<br>*ON                      | 6         |
| Anzeige, ob die Benutzerkennung schaltbar ist                                                         | var(*LIST).USER-AUDIT(*LIST).<br>SWITCHABLE   | B | FALSE<br>TRUE                    | 6         |
| Benutzerkennung, für die die Protokollierung eingeschaltet ist                                        | var(*LIST).USER-AUDIT(*LIST).<br>USER-ID      | S | <name 1..8>                      | 6         |

(Teil 2 von 2)

## SHOW-SAT-SUPPORT-PARAMETERS

### Einstellung der produktspezifischen Protokollierung und Alarmauslösung anzeigen

**Anwendungsbereich:** SECURITY-ADMINISTRATION

**Privilegierung:** SECURITY-ADMINISTRATION

Mit dem Kommando /SHOW-SAT-SUPPORT-PARAMETERS können sich der Sicherheitsbeauftragte, der SAT-Datei-Verwalter und der SAT-Datei-Auswerter darüber informieren für welches Produkt die SAT-Protokollierung und die Auslösung der SAT-Alarme generell aktiviert oder deaktiviert ist.

#### SHOW-SAT-SUPPORT-PARAMETERS

```
VALUE = *CURRENT / *STD / *NEXT-SESSION
,OUTPUT = *SYSOUT / *SYSLST(...)
  *SYSLST(...)
    | LINES-PER-PAGE = 64 / <integer 20..255>
```

#### VALUE =

Legt fest, welche Information ausgegeben wird.

#### VALUE = \*CURRENT

Die momentan gültigen Werte werden ausgegeben.

#### VALUE = \*STD

Die Standardwerte werden ausgegeben.

#### VALUE = \*NEXT-SESSION

Die in der nächsten Sitzung gültigen Werte werden ausgegeben.

#### OUTPUT = \*SYSOUT

Die angeforderte Information wird auf SYSOUT ausgegeben.

#### OUTPUT = \*SYSLST(...)

Die angeforderte Information wird auf SYSLST ausgegeben.

#### LINES-PER-PAGE = 64 / <integer 20..255>

Bestimmt die Zeilenzahl der Ausgabeseite.

**Kommando-Returncode**

| (SC2) | SC1 | Maincode | Bedeutung                                                                  |
|-------|-----|----------|----------------------------------------------------------------------------|
|       | 0   | CMD0001  | Kommando erfolgreich ausgeführt                                            |
|       | 32  | CMD2009  | Systemfehler bei Ausgabe der S-Variablen                                   |
|       | 32  | SAT0000  | Nicht behebbarer Fehler.<br>SATCP ist evtl. in einem inkonsistenten Status |
|       | 32  | SAT5000  | Nicht behebbarer Fehler                                                    |
|       | 64  | OPS0002  | Ausgabe der S-Variablen wurde unterbrochen                                 |
|       | 64  | SAT1000  | Benutzer für Kommando nicht privilegiert                                   |
|       | 64  | SAT5001  | Speicherzuweisung für SYSLST-Datei nicht ausreichend                       |
|       | 130 | CMD2009  | OPS nicht verfügbar                                                        |
|       | 130 | OPS0001  | Ausgabe der S-Variablen konnte nicht durchgeführt werden                   |
|       | 130 | SAT1010  | Anderes Kommando wird derzeit ausgeführt                                   |
|       | 130 | SAT1080  | Wechsel in Vorbereitung                                                    |
|       | 130 | SAT4010  | SAT-Parameterdatei derzeit nicht verfügbar                                 |

**Ausgabe in S-Variablen**

| Ausgabe-Information              | Name der S-Variablen    | T | Inhalt                | Bedingung |
|----------------------------------|-------------------------|---|-----------------------|-----------|
| SAT-Support für POSIX-Ereignisse | var(*LIST).POSIX-EVENTS | S | *ENABLED<br>*DISABLED |           |

*Beispiel*

Der Benutzer modifiziert den SAT-Support für POSIX-Ereignisse und möchte sich anschließend über die durchgeführten Änderungen informieren.

```
/modify-sat-support-parameters posix-events=*enabled
/show-sat-support-parameters
```

```
SAT support for POSIX events : ENABLED
```

## 2.6 SATUT – SATLOG-Dateien auswerten

Die Aufbereitung der SATLOG-Dateien ist Aufgabe der SAT-Datei-Verwaltung oder der SAT-Datei-Auswertung. Für die Auswertung steht das Dienstprogramm SATUT unter der Kennung SYSAUDIT zur Verfügung.

Es ist unabhängig vom SAT-Subsystem SATCP unter jeder Benutzerkennung ablauffähig, die das Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION besitzt.

SATUT kann neben SATLOG-Dateien auch CONSLOG-Dateien (siehe [Seite 221](#)) in die Auswertung einbeziehen.

Der SAT-Auswerter SATUT dient dazu,

- aus den Eingabedateien aufbereitete Dateien (replacement-files) zu erstellen, in der die sicherheitsrelevanten Aufzeichnungen stehen, die die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung ausgewählt hat. In diesem Fall ist das Ziel die Reduktion der Datenmenge und Aufbewahrung der sicherheitsrelevanten SATLOG-Sätze, d.h. die Eingabedateien können durch die aufbereiteten Dateien ersetzt werden.
- aus den Eingabedateien mit Auswahlbedingungen bestimmte Protokoll Datensätze auszuwählen. Diese werden auf Drucker (SYSLST) oder in eine XML-Datei ausgegeben, statistisch dargestellt oder in eine Datei (analysis-file) geschrieben. In diesem Fall ist das Ziel die Analyse ausgewählter Ereignisgruppen, d.h. die Eingabedateien werden nicht durch die aufbereiteten Dateien ersetzt.

### 2.6.1 Arbeiten mit SATUT

Zum Erstellen der aufbereiteten Protokolldateien stellt SATUT folgende Grundfunktionen in Form von Anweisungen zur Verfügung:

1. Eine Anweisung zur Festlegung der Eingabedateien für den SATUT-Lauf (//SELECT-INPUT-FILES).
2. Anweisungen zur Festlegung von Auswahlbedingungen für die Aufbereitung (//ADD-, //REMOVE-, //SHOW-SELECTION-CONDITIONS).
3. Eine Anweisung zur Durchführung der Selektion in Abhängigkeit von den Auswahlbedingungen (//START-SELECTION).
4. Anweisungen, mit denen die selektierten Datensätze auf Drucker (SYSLST), in eine XML-Datei oder in statistischer Form ausgegeben werden (//SHOW-SELECTED-RECORDS, //SHOW-STATISTICS).
5. Eine Anweisung, mit der selektierte Datensätze in reduzierte SAT-Protokolldateien geschrieben werden können (//SAVE-SELECTED-RECORDS).

Die Reihenfolge der Funktionen entspricht auch dem Schema einer Auswertung mit SATUT. Die Funktionen 2. bis 5. können dabei mehrfach ausgeführt werden.

## 2.6.2 Eingabedateien für SATUT

Als Eingabedateien für den SAT-Auswerter SATUT werden folgende Dateien akzeptiert:

- SATLOG-Dateien (\$SYSAUDIT.SYS.SATLOG.yyyy-mm-dd.sss.nn)
- reduzierte SAT-Protokolldateien mit Standardnamen (replacement-files) (\$SYSAUDIT.SYS.SATUT.yyyy-mm-dd.sss.nnn)
- CONSLOG-Dateien (mit Standardnamen)

Die gleichzeitige Eingabe von replacement-files und einer oder mehrerer Eingabedateien, aus denen diese entstanden sind, ist nicht erlaubt, da hier Überlappungen vorkommen.

Alternativ zu obiger Liste können reduzierte SAT-Protokolldateien ohne Standardnamen (analysis-files) angegeben werden.

Bei Eingabe von analysis-files können gleiche Datensätze mehrfach vorkommen und die Analyse (besonders bei Statistiken) verfälschen.

## 2.6.3 Arbeitsdateien im SATUT-Lauf

Die zu selektierenden Datensätze werden mit der Anweisung //START-SELECTION zunächst pro Selektionsbedingung in einer SATUT-Arbeitsdatei zwischengespeichert. Bis zu zehn solcher Arbeitsdateien (0..9) stehen in einem SATUT-Lauf zur Verfügung.

Der Inhalt dieser Arbeitsdateien kann dann

- ausgegeben werden (siehe nächster Abschnitt) oder
- als Eingabe für ein weiteres START-SELECTION-Kommando dienen

## 2.6.4 Ausgabe von SATUT

Die selektierten Datensätze werden wahlweise ausgegeben

- in lesbarer Form auf SYSLST oder in eine XML-Datei (//SHOW-SELECTED-RECORDS)
- in statistischer Form auf SYSOUT oder SYSLST (//SHOW-STATISTICS)
- in Originalform in reduzierte SAT-Protokolldateien mit Standardnamen (replacement-files) oder ohne Standardnamen (analysis-files) (//SAVE-SELECTED-RECORDS)

Zur Archivierung und Analyse sicherheitsrelevanter Daten erstellt SATUT zwei Typen reduzierter SAT-Protokolldateien: **replacement-files** und **analysis-files**.

Replacement- und analysis-files enthalten die gleiche Art von Information. Sie sind das Ergebnis eines oder mehrerer Selektionsvorgänge eines SATUT-Laufes. Sie unterscheiden sich in ihrem Verwendungszweck und der Namensgebung.

Neben der Nutzinformation enthalten beide Dateitypen Zusatzinformationen, die mit der Anweisung //SHOW-REDUCTION-FILES-ORIGIN ausgegeben werden können:

- Erstellungsdatum dieser Datei
- die Auswahl-Bedingung
- die Eingabedateien, aus denen die Datensätze ausgewählt wurden

### Replacement-files

Replacement-files enthalten die sicherheitsrelevanten Informationen aus den Eingabedateien, die die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung zur **Archivierung** ausgewählt hat.

Replacement-files dienen der Aufbewahrung sicherheitsrelevanter Protokolldatensätze (SATLOG sowie in konvertierter Form CONSLOG) und einer eventuellen erneuten Eingabe in einem Auswertungslauf.

Sie ersetzen normalerweise die Eingabedateien, aus denen sie erzeugt wurden. Beim Erstellen der replacement-file kann die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung entscheiden, ob sie die Eingabedateien löschen will, falls es sich dabei ausschließlich um SATLOG-Dateien handelt.

Wenn die replacement-files die Eingabedateien ersetzen sollen, sollten nur komplette SATLOG-Dateien oder replacement-files aufbereitet werden.

Mit der Anweisung SAVE-SELECTED RECORDS wird eine replacement-file unter der Benutzerkennung SYSAUDIT abgelegt. Dazu muss der SATUT-Lauf ebenfalls unter SYSAUDIT stattfinden.

Replacement-files haben einen Standardnamen:

`$$SYSAUDIT.SYS.SATUT.yyyy-mm-dd.sss.nnn` wobei:

|            |                                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| yyyy-mm-dd | Erstellungsdatum der (zeitlich) ersten Datei der Eingabedateien, aus denen die replacement-file erzeugt wurde. Eingabedateien können sein: SATLOG-Dateien, replacement-files, CONSLOG-Dateien. |
| sss        | session-number                                                                                                                                                                                 |
| nnn        | Folgenummer der Datei (001..999)                                                                                                                                                               |

### **Analysis-files**

Analysis-files enthalten die sicherheitsrelevanten Informationen aus den Eingabedateien, die die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung zur **Analyse** ausgewählt hat. Analysis-files dienen der dezentralen Analyse sicherheitsrelevanter Protokolldatensätze (SATLOG sowie in konvertierter Form CONSLOG).

Analysis-files ersetzen nicht die Eingabedateien, aus denen sie erzeugt werden.

Mit der Anweisung //SAVE-SELECTED RECORDS wird eine analysis-file unter der Benutzerkennung abgelegt, in der auch der SATUT-Lauf stattfindet.

Im Gegensatz zur replacement-file kann die analysis-file somit unter jeder anderen Benutzerkennung mit dem Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION angelegt werden.

Ihr Name kann frei gewählt werden.

## 2.6.5 SATUT starten

SATUT wird mit dem Kommando /START-SATUT gestartet und mit der Anweisung END beendet.

Aus Kompatibilität werden noch die Kommandos /START-EVALUATOR, /START-EVALU, /EVALUATOR und /SATUT zum Starten von SATUT unterstützt.

### START-SATUT

#### Auswertung der SATLOG-Dateien einleiten

**Anwendungsbereich:** UTILITIES, SECURITY-ADMINISTRATION

**Privilegierung:** SAT-FILE-MANAGEMENT, SAT-FILE-EVALUATION

#### START-SATUT

**VERSION** = \*STD / <product-version>

**,MONJV** = \*NONE / <filename 1..54 without-gen-vers>

**,CPU-LIMIT** = \*JOB-REST / <integer 1..32767 seconds>

**VERSION = \*STD / <product-version>**

Version von SATUT, die gestartet wird.

**VERSION = \*STD**

Die mit dem Kommando /SELECT-PRODUCT-VERSION eingestellte Version wird als Standardversion verwendet.

**VERSION = <product-version>**

Explizite Angabe der Version.

**MONJV = \*NONE / <filename 1..54 without-gen-vers>**

Angabe einer Monitor-Jobvariablen zur Überwachung des SATUT-Laufs.

**MONJV = \*NONE**

Es wird keine Monitor-Jobvariable verwendet.

**MONJV = <filename 1..54 without-gen-vers>**

Name der zu verwendenden Jobvariablen.

**CPU-LIMIT = \*JOB-REST / <integer 1..32767 seconds>**

Maximale CPU-Zeit in Sekunden, die das Programm bei Ablauf verbrauchen darf.

**CPU-LIMIT = \*JOB-REST**

Es soll die verbleibende CPU-Zeit für die Task verwendet werden.

**CPU-LIMIT = <integer 1..32767 seconds>**

Es soll nur die angegebene Zeit verwendet werden.

*Hinweis*

Die überwachende Jobvariable kann folgende Werte annehmen:

- 0000 Kein Fehler
- 1010 Fehlerhafte Anweisung oder unerwartete END-Anweisung.  
Ergebnisse können fehlerhaft oder unvollständig sein.
- 1020 Benutzer besitzt kein Privileg zum Starten von SATUT
- 1030 Eingabedateien nicht vorhanden
- 2010 Fehlerhafte Anweisung. Ergebnisse können fehlerhaft oder unvollständig sein.
- 2015 Unerwartetes Dateiende auf SYSDDTA, SATUT beendet
- 3020 Interne Inkonsistenz, SATUT mit Dump beendet

## 2.6.6 SATUT-Anweisungen

In diesem Kapitel werden alle SATUT-Anweisungen in alphabetischer Reihenfolge aufgeführt. Die Beschreibung der Anweisungen ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion der Anweisung erklärt, dann folgt das Anweisungsformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung folgt gegebenenfalls ein Anwendungsbeispiel.

Die Metasyntax zu den Anweisungen finden Sie im Anhang des Handbuchs.

### Funktionelle Übersicht

#### SATUT starten und beenden

|                        |                                         |
|------------------------|-----------------------------------------|
| START-SATUT (Kommando) | Auswertung der SATLOG-Dateien einleiten |
| END                    | Auswertung beenden                      |

#### Eingabedateien festlegen

|                             |                                         |
|-----------------------------|-----------------------------------------|
| SHOW-REDUCTION-FILES-ORIGIN | Herkunft von replacement-files anzeigen |
| SELECT-INPUT-FILES          | Eingabedateien für SATUT festlegen      |

#### Auswahlbedingungen festlegen und Datensätze auswählen

|                             |                                                            |
|-----------------------------|------------------------------------------------------------|
| ADD-SELECTION-CONDITIONS    | Auswahlbedingungen festlegen                               |
| REMOVE-SELECTION-CONDITIONS | Auswahlbedingungen entfernen                               |
| SHOW-SELECTION-CONDITIONS   | Auswahlbedingungen anzeigen                                |
| START-SELECTION             | Auswahl unter Beachtung der Auswahlbedingungen durchführen |

#### Aufbereitete Dateien sichern und analysieren

|                       |                                                                   |
|-----------------------|-------------------------------------------------------------------|
| SAVE-SELECTED-RECORDS | Ausgewählte Datensätze in replacement-/analysis-files sichern     |
| SHOW-SELECTED-RECORDS | Ausgewählte Datensätze auf SYSLST oder in eine XML-Datei ausgeben |
| SHOW-STATISTICS       | SAT-Statistiken auf SYSLST oder SYSOUT ausgeben                   |

### Datensätze nach Auswahlbedingungen auswählen

(wird nur noch aus Kompatibilität unterstützt; stattdessen sind die Anweisungen //ADD-SELECTION-CONDITIONS, //REMOVE-SELECTION-CONDITIONS, //SHOW-SELECTION-CONDITIONS und //START-SELECTION zu verwenden)

|                |                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------|
| SELECT-RECORDS | Aufbereitungsbedingung festlegen<br>Sätze nach bestimmten Aufbereitungs-<br>bedingungen aussuchen |
|----------------|---------------------------------------------------------------------------------------------------|

### Abfolge der Anweisungen

Bei den folgenden Anweisungen ist die Eingabereihenfolge zu beachten, da sie aufeinander aufbauen. Die Schritte 2-4 können in einem Auswertungslauf mehrfach angegeben werden. Die übrigen Anweisungen von SATUT können wahlfrei im Auswertungslauf angegeben werden.

1. //SELECT-INPUT-FILES zur Definition der Eingabedaten.
2. //ADD-SELECTION-CONDITIONS zur Definition der Selektionsbedingungen.
3. //START-SELECTION zur Durchführung der Datenselektion.
4. //SHOW-SELECTED-RECORD, //SHOW-STATISTICS, //SAVE-SELECTED-RECORDS zum Betrachten und Sichern der selektierten Daten.

## ADD-SELECTION-CONDITIONS

### Auswahlbedingungen festlegen

Mit der Anweisung //ADD-SELECTION-CONDITIONS wird eine Auswahlbedingung für Protokolldatensätze festgelegt und benannt. In der Auswahlbedingung ist Wildcard-Syntax möglich.

#### ADD-SELECTION-CONDITIONS

**NAME** = <name 1..8>

**CONDITION** = \*NONE / <text 1..1800 with-low>

#### **NAME = <name 1..8>**

Name der Auswahlbedingung, die im Operanden CONDITION festgelegt ist.

#### **CONDITION = \*NONE / <text 1..1800>**

Die Auswahlbedingungen werden festgelegt.

#### **CONDITION = \*NONE**

Die Auswahl ist uneingeschränkt.

#### **CONDITION = <text 1..1800 with-low>**

Die Auswahlbedingung besteht aus einem oder mehreren logischen Ausdrücken, die durch die logischen Operatoren AND, OR und NOT verknüpft werden. Zusätzlich kann durch Klammerung „(...)“ die Reihenfolge der Auswertung der Ausdrücke festgelegt werden. Die Operatoren werden auf logische Ausdrücke angewendet, die die Wahrheitswerte „TRUE“ oder „FALSE“ annehmen können (siehe Wahrheitstafeln). Es werden die Datensätze ausgewählt, die die Bedingung erfüllen.

Die Auswahlbedingung wird bei <text 1..1800 with-low> in folgender Weise angegeben:

```
[NOT] cond1 [OR/AND [NOT] cond2...]
```

Mit der Auswahlbedingung kann:

- a) innerhalb einer Liste gesucht werden,
- b) innerhalb eines Bereichs gesucht werden,
- c) mit einem Wert verglichen werden.
- d) geprüft werden, ob ein Feld vorhanden ist
- e) mit Wildcard-Syntax gesucht werden



Im Allgemeinen werden Klein- und Großbuchstaben in der Auswahlbedingung gleich behandelt. Eine Unterscheidung findet nur bei Werteangaben für die folgenden Feldnamen statt: homedir, linknam, newpath, pathnam, shell und symbdev.

Dementsprechend kann *cond* Folgendes sein:

- a) Suchen innerhalb einer Liste

```
field-name IN-LIST/NOT-IN-LIST (value,...)
```

```
field-name IN-LIST (value1,...valuen)
```

Ein Datensatz wird ausgewählt, wenn das angegebene Feld vorhanden ist und wenn dessen Inhalt einem der angegebenen Werte entspricht.

```
field-name NOT-IN-LIST (value1,...valuen)
```

Ein Datensatz wird ausgewählt, wenn im angegebenen Feld keiner der angegebenen Werte steht oder wenn das angegebene Feld nicht vorhanden ist.

- b) Suchen innerhalb eines Bereichs

```
field-name IN-RANGE/NOT-IN-RANGE (value-range)
```

```
field-name IN-RANGE (value:value)
```

Ein Datensatz wird ausgewählt, wenn das angegebene Feld vorhanden ist und wenn dessen Inhalt einem Wert im angegebenen Bereich entspricht. Es werden nur das Feld *timestp* (Format: yyyy-mm-dd/hh:mm:ss) und Felder mit dem SDF-Datentyp *integer* akzeptiert.

```
field-name NOT-IN-RANGE (value:value)
```

Ein Datensatz wird ausgewählt, wenn im angegebenen Feld kein Wert des angegebenen Bereichs steht oder wenn das Feld nicht vorhanden ist. Es werden nur das Feld *timestp* (Format: yyyy-mm-dd/hh:mm:ss) und Felder mit dem SDF-Datentyp *integer* akzeptiert.

## c) Vergleichen mit einem Wert

field-name EQUAL/NOT-EQUAL value

field-name EQUAL value

Ein Datensatz wird ausgewählt, wenn das angegebene Feld vorhanden ist und den angegebenen Wert enthält.

field-name NOT-EQUAL value

Ein Datensatz wird ausgewählt, wenn im angegebenen Feld ein anderer als der angegebene Wert steht oder wenn das angegebene Feld nicht vorhanden ist.

## d) Suchen eines bestimmten Feldnamens

field-name PRESENT

Alle Datensätze, die das angegebene Feld enthalten, werden ausgewählt.

## e) Mit Wildcard-Syntax suchen

field-name MATCH/NOT-MATCH pattern

field-name MATCH pattern

Alle Datensätze, die dem angegebenen Suchmuster entsprechen, werden ausgewählt. Es werden nur Felder mit dem SDF-Datentyp c-string mit Ausnahme von plamrc akzeptiert.

field-name NOT-MATCH pattern

Alle Datensätze, die dem angegebenen Suchmuster nicht entsprechen, werden ausgewählt. Es werden nur Felder mit dem SDF-Datentyp c-string mit Ausnahme von plamrc akzeptiert.

**Definitionen**

field-name bezeichnet die Typen der protokollierbaren Information z.B. access, acckey,... (siehe Tabelle auf [Seite 279](#)). Andere Angaben werden als Fehler abgewiesen. Die Angabe des Namens eines \*LNG-Feldes (siehe [Seite 51](#)) für field-name ist nicht erlaubt.

value entspricht den in SDF definierten Datentypen: <x-string>, <c-string>, <integer>, <keyword>. value muss dem Datentyp entsprechen, der bei dem zugehörigen field-name angegeben ist (siehe Tabelle auf [Seite 279](#)). Z.B. gehört zum Feldnamen dmsrc ein value vom Typ x-string.

**Besonderheit bei field-name = filpos / curlim2 / maxlim2:**

Für die Feldnamen filpos, curlim2 und maxlim2 existiert ein spezieller Datentyp <integer-with-unit>. Dieser unterscheidet sich vom Datentyp <integer> dadurch, dass zusätzlich in Klammern eine Maßeinheit angegeben

werden kann, also <integer>( <unit>). <unit> kann BYTES, KB (=Kilobytes), MB (=Megabytes) oder GB (=Gigabytes) sein. Fehlt die Angabe, wird BYTES angenommen.

- Falls als Maßeinheit explizit oder implizit BYTES festgelegt ist, muss der Zahlenwert ein Vielfaches von 512 sein. Anderenfalls wird die Anweisung mit einer Fehlermeldung abgewiesen.
- Die Angabe eines Zahlenwertes mit Maßeinheit wird intern immer in Vielfache von 512 Bytes umgerechnet. Nur dieser Wert ist für das Ergebnis einer Auswahlbedingung von Belang, nicht jedoch die Form der Eingabe. Z.B. werden die Angaben 3145728(BYTES), 3072(KB) und 3(MB) als gleichwertig betrachtet, da jede denselben Wert von 3145728 Bytes darstellt.
- Unabhängig von der UNIT-Angabe darf der Maximalwert von  $2^{40}-512$  (=1 099 511 627 264) Bytes nicht überschritten werden. Damit ergeben sich für die jeweiligen UNIT-Angaben folgende Maximalwerte:

| UNIT         | Maximaler Zahlenwert          | entspricht in Bytes                     |
|--------------|-------------------------------|-----------------------------------------|
| <b>BYTES</b> | $2^{31}-1 = 2\ 147\ 483\ 647$ | $2^{31}-1 = 2\ 147\ 483\ 647$           |
| <b>KB</b>    | $2^{30}-1 = 1\ 073\ 741\ 823$ | $2^{40}-2^{10} = 1\ 099\ 511\ 626\ 752$ |
| <b>MB</b>    | $2^{20}-1 = 1\ 048\ 575$      | $2^{40}-2^{20} = 1\ 099\ 510\ 579\ 200$ |
| <b>GB</b>    | $2^{10}-1 = 1\ 023$           | $2^{40}-2^{30} = 1\ 098\ 437\ 885\ 952$ |

value-range bezeichnet einen Bereich von Werten, der sich wie folgt zusammensetzt: <value:value>.

pattern bezeichnet einen c-string, bei dem analog zum SDF-Datentyp <c-string with-wild (n)> Teile der Zeichenfolge durch Platzhalter (wildcards) ersetzt werden können. pattern darf höchstens 281 Zeichen lang sein. Die zur Verfügung stehenden Wildcard-Zeichen sind:

- \* Ersetzt eine beliebige, auch leere Zeichenfolge.
- / Ersetzt genau ein beliebiges Zeichen.
- \ Entwertet Platzhalter (\* / < > : ,) in einer Zeichenfolge (z.B. ab\\*c bezeichnet die Zeichenfolge „ab\*c“).

<s<sub>x</sub>:s<sub>y</sub>> Ersetzt eine Zeichenfolge für die gilt:

- Sie ist mindestens so lang wie die kürzeste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
- Sie ist höchstens so lang wie die längste Zeichenfolge (s<sub>x</sub> oder s<sub>y</sub>).
- Sie liegt in der alphabetischen Sortierung zwischen s<sub>x</sub> und s<sub>y</sub>; Zahlen werden hinter Buchstaben sortiert (A...Z 0...9).
- s<sub>x</sub> darf auch die leere Zeichenfolge sein, die in alphabetischer Sortierung an erster Stelle steht.
- s<sub>y</sub> darf auch die leere Zeichenfolge sein, die an dieser Stelle für die Zeichenfolge mit der höchsten möglichen Codierung steht (enthält nur die Zeichen X'FF').
- s<sub>x</sub> muss in der alphabetischen Sortierung vor s<sub>y</sub> stehen. Ist s<sub>x</sub> kürzer als s<sub>y</sub> wird s<sub>x</sub> mit X'00' aufgefüllt.
- Ist s<sub>y</sub> kürzer als s<sub>x</sub> wird s<sub>y</sub> mit X'FF' aufgefüllt.
- Weder in s<sub>x</sub> noch in s<sub>y</sub> dürfen Platzhalter vorkommen.

<s1,...> Ersetzt alle Zeichenfolgen, auf die eine der mit s angegebenen Zeichenkombinationen zutrifft. s kann auch eine leere Zeichenfolge sein. Jede Zeichenfolge s kann auch eine Bereichsangabe <s<sub>x</sub>:s<sub>y</sub>> sein.

Der Platzhalter „-“ zur Verneinung einer Aussage wird hier nicht verwendet. Dafür ist NOT-MATCH vorgesehen.

### *Hinweise*

1. Wird bei der syntaktischen Analyse der Anweisung ein Fehler entdeckt, wird die Auswahlbedingung auf SYSOUT ausgegeben. An der fehlerhaften Stelle befindet sich dann ein Fragezeichen.
2. Wenn der Benutzer im geführten Dialog arbeitet, führt die oben genannte Ausgabe auf SYSOUT zum Verlust des SDF-Bildschirms. Mit der Anweisung //RESTORE-SDF-INPUT wird der SDF-Bildschirm wieder hergestellt.
3. Posix-filenames und Kerberos-Namen werden von SAT ohne Einschränkung protokolliert. Bei der Definition von Auswahlbedingungen wird die Groß- und Kleinschreibung bei folgenden SAT-Feldern unterstützt: AUDITID, HOMEDIR, LINKNAM, NEWPATH, PATHNAM, PRINCCL, PRINCSV, SHELL, SYMBDEV. Bei den Feldern, für die nicht zwischen Groß- und Kleinbuchstaben unterschieden wird, erfolgt intern eine Umwandlung nach Großbuchstaben. Die Felder können mit Ausnahme von SYMBDEV allerdings nur in einer Länge von max. 255 Bytes angegeben werden. Events mit längeren Feldinhalten

ten können durch die Angabe von Wildcards selektiert werden. Für die Angabe eines Einzelnamens (ohne Wildcards) werden Sonderzeichen zugelassen, wie sie für posix-filenames bzw. für Kerberos-Namen erlaubt sind.

### Beispiele

```
//add-selection-conditions name = filese1, -
//          condition = filename in-list ('filex','filey') - - (1)
//          and access equal input - _____ (2)
//          and res      equal f - _____ (3)
//          and dmsrc   equal x'0d35' - _____ (4)
```

Unter der Bedingung mit dem Namen filese1 werden Ereignisse ausgewählt, wenn

- (1) die Dateien 'FILEX' oder 'FILEY' betroffen sind **und**
- (2) der Open-Modus INPUT ist **und**
- (3) das Ergebnis der Operation 'failure' ist **und**
- (4) die Datei nicht mehrbenutzbar ist (DMS Return Code 0D35).

```
//add-selection-conditions name = groupse1, -
//          condition = (groupid equal c'g1' - _____ (1)
//          and not auditid present) - _____ (2)
//          or (groupid in-list (c'g2',c'g3') - _____ (3)
//          and user-id not-in-list ('u1','u2')) (4)
```

Unter der Bedingung mit dem Namen groupse1 werden Ereignisse ausgewählt, wenn sie

- (1) von Benutzern der Gruppenkennung G1 erzeugt wurden **und** diese sich **nicht**
- (2) mit einer Chipkarte oder mit einer persönlichen Benutzerkennung gegenüber dem System identifiziert haben **oder**
- (3) von Benutzern der Gruppenkennungen G2 ODER G3 erzeugt wurden **und**
- (4) diese nicht die Benutzerkennung U1 bzw. U2 haben.

```
//add-selection-conditions name = satsel, -
// condition = evt equal 'FRD' -
//          and filename match '$sysaudit.sys.satlog.*' -
//          and timestp in-range (2017-05-01/00:00:00 : 2017-05-31/23:59:59) -
//          and userid not-in-list ('tsos','sysaudit')
```

Unter der Bedingung mit dem Namen satsel werden Lesezugriffe nicht-privilegierter Benutzerkennungen auf SATLOG-Dateien im Mai 2017 ausgewählt.

**Wahrheitstafeln**

Für AND, OR und NOT gelten folgende Wahrheitstafeln:

| <b>cond1</b> | <b>AND</b> | <b>cond2</b> | <b>TRUE</b> | <b>FALSE</b> |
|--------------|------------|--------------|-------------|--------------|
| TRUE         |            |              | TRUE        | FALSE        |
| FALSE        |            |              | FALSE       | FALSE        |

| <b>cond1</b> | <b>OR</b> | <b>cond2</b> | <b>TRUE</b> | <b>FALSE</b> |
|--------------|-----------|--------------|-------------|--------------|
| TRUE         |           |              | TRUE        | TRUE         |
| FALSE        |           |              | TRUE        | FALSE        |

| <b>cond1</b> | <b>TRUE</b> | <b>FALSE</b> |
|--------------|-------------|--------------|
| NOT cond1    | FALSE       | TRUE         |

Gleiche Operatoren werden von links nach rechts abgearbeitet.

## END

### Auswertung beenden

Die Anweisung //END beendet die Auswertung mit SATUT.

|     |
|-----|
| END |
|     |

Diese Anweisung hat keine Operanden.

## REMOVE-SELECTION-CONDITIONS

### Auswahlbedingungen entfernen

Mit der Anweisung //REMOVE-SELECTION-CONDITIONS werden eine oder mehrere Auswahlbedingungen (siehe //ADD-SELECTION-CONDITIONS) entfernt.

|                                                        |
|--------------------------------------------------------|
| REMOVE-SELECTION-CONDITIONS                            |
| <b>NAME</b> = <u>*ALL</u> / list-poss(10): <name 1..8> |

**NAME** = \*ALL / list-poss(10): <name 1..8>

Angabe der Auswahlbedingungen, die entfernt werden sollen.

**NAME** = \*ALL

Alle definierten Auswahlbedingungen sollen entfernt werden.

**NAME** = list-poss(10): <name 1..8>

Explizite Angabe von Auswahlbedingungen, die entfernt werden sollen.

## SAVE-SELECTED-RECORDS

### Ausgewählte Datensätze sichern

Mit der Anweisung //SAVE-SELECTED-RECORDS werden die durch die Aufbereitung (//START-SELECTION bzw. //SELECT-RECORDS) erstellten Datensätze in eine replacement-file oder eine analysis-file gesichert.

#### SAVE-SELECTED-RECORDS

**TO-REDUCTION-NAME** = **\*STD** / <filename 1..38 without-cat-user-gen>  
**,FROM-FILE** = **0** / <integer 0..9>  
**,ERASE-INPUT-FILES** = **\*NO** / \*YES

#### **TO-REDUCTION-NAME =**

Bestimmt, ob eine replacement-file oder eine analysis-file erzeugt werden soll.

#### **TO-REDUCTION-NAME = \*STD**

Es wird eine replacement-file mit Standarddateinamen unter der Standard-Katalogkennung (DEFAULT-CATID) der Benutzerkennung SYSAUDIT erzeugt.

Replacement-files können nur erzeugt werden, wenn SATUT unter der Benutzerkennung SYSAUDIT läuft.

#### **TO-REDUCTION-NAME = <filename 1..38 without-cat-user-gen>**

Es wird eine analysis-file auf der aktuellen Benutzerkennung erzeugt.

#### **FROM-FILE = 0 / <integer 0..9>**

Arbeitsdatei, deren Inhalt gesichert wird.

#### **ERASE-INPUT-FILES = \*NO / \*YES**

Bestimmt, ob Eingabedateien gelöscht werden.

#### **ERASE-INPUT-FILES = \*NO**

Die Eingabedateien werden nicht gelöscht.

#### **ERASE-INPUT-FILES = \*YES**

Diese Angabe ist nur erlaubt, wenn mit TO-REDUCTION-NAME=\*STD eine replacement-file erzeugt wird und SATUT unter der Benutzerkennung SYSAUDIT läuft.

Die Eingabedateien des SATUT-Laufes werden gelöscht.

Ausnahmen:

CONSLOG-Dateien sowie Eingabedateien, die mit

//SELECT-INPUT-FILES ..., STATUS=NOT-CLOSED ausgewählt wurden, werden nicht gelöscht.

*Hinweise*

1. Existiert die zu erzeugende replacement-/analysis-file bereits, muss die SAT-Datei-Verwaltung oder SAT-Datei-Auswertung im Dialog entscheiden, ob die Datei überschrieben werden soll oder nicht.  
In einem Batch-Job wird in diesem Fall die Ausführung der Anweisung abgebrochen.
2. Aus Eingabedateien, die nicht den Standarddateinamen besitzen (analysis-files), können keine replacement-files erzeugt werden, da für die replacement-files sonst kein den Regeln entsprechender Name gebildet werden kann. In diesem Fall wird eine Fehlermeldung ausgegeben und die Ausführung der Anweisung abgebrochen.

*Beispiel*

Die SAT-Datei-Verwaltung will SATLOG-Dateien durch eine einzige replacement-file ersetzen. Dazu definiert sie mit der Anweisung //SELECT-INPUT-FILES die Eingabedateien, führt die Selektion in die Arbeitsdatei 0 durch (//START-SELECTION) und gibt dann folgende Anweisung:

```
//save-selected-records from-file=0, to-reduction-name=*std, -  
//                               erase-input-files=*yes
```

oder in Kurzform:

```
//save-sel-rec erase-input-files=*y
```

Mit dieser Anweisung wird die Arbeitsdatei 0 als replacement-file mit Standarddateinamen gesichert.

## SELECT-INPUT-FILES

### Eingabedateien festlegen

Mit der Anweisung //SELECT-INPUT-FILES werden die zu bearbeitenden Dateien ausgewählt. Die Anweisung kann je SATUT-Lauf nur einmal angegeben werden.

#### SELECT-INPUT-FILES

```

INPUT-FILES = *STD(...) / list-poss(100): <filename 1..54>
  *STD(...)
    TYPE = list-poss(3): *SAT / *CONSLOG
    ,STATUS = *CLOSED / *NOT-CLOSED / *ALL
    ,PUBSET = *STD / list-poss(20): <cat-id 1..4>
    ,DATE = *ALL / <date 8..10> / *INTERVAL(...)
      *INTERVAL(...)
        FIRST-DATE = <date 8..10>
        ,LAST-DATE = <date 8..10>
    ,SESSION-NUMBER = *ALL / <integer 1..999> / *RANGE(...)
      *RANGE(...)
        FIRST-SESSION-NUMBER = <integer 1..999>
        ,LAST-SESSION-NUMBER = <integer 1..999>
    ,SEQUENCE-NUMBER = *ALL / <integer 1..999> / *RANGE(...)
      *RANGE(...)
        FIRST-SEQU-NUMBER = <integer 1..999>
        ,LAST-SEQU-NUMBER = <integer 1..999>

```

#### **INPUT-FILES =**

Bestimmt die Dateitypen, die als Eingabe für die Aufbereitung dienen.

**INPUT-FILES = \*STD(...)**

Nur Dateien mit Standardnamen (SATLOG-Dateien, replacement-files und CONSLOG-Dateien) werden als Eingabe für diesen SATUT-Lauf verwendet.

**TYPE = list-poss(3): \*SAT / \*CONSLOG**

Bestimmt die Dateitypen, die ausgewählt werden.

**TYPE = \*SAT**

Als Eingabedateien werden SATLOG-Dateien und replacement-files genommen.

**TYPE = \*CONSLOG**

Als Eingabedateien werden CONSLOG-Dateien genommen.

**STATUS =**

Bestimmt den Zustand der Eingabedatei.

**STATUS = \*CLOSED**

Die angegebene Datei muss geschlossen sein.

**STATUS = \*NOT-CLOSED**

Die angegebene Datei darf nicht geschlossen sein.

**STATUS = \*ALL**

Jeder Zustand der angegebenen Datei ist zugelassen.

**PUBSET =**

bezeichnet den Pubset, auf dem SATUT die angegebenen Dateien sucht.

Aus Kompatibilitätsgründen sind die Angaben PUBLIC-VOLUME-SET oder PUB-VOL-SET an Stelle von PUBSET noch zugelassen.

**PUBSET = \*STD**

SATUT sucht die angegebenen Dateien auf dem Standard-Pubset (DEFAULT-CATID) der Benutzerkennung SYSAUDIT.

**PUBSET = list-poss(20): <cat-id 1..4>**

SATUT sucht die angegebenen Dateien auf den angegebenen Pubsets.

**DATE =**

Bestimmt, welches Datum die Eingabedateien haben sollen.

**DATE = \*ALL**

Jedes Datum im Standardnamen der Eingabedatei ist zugelassen.

**DATE = <date 8..10>**

Erstellungsdatum, das im Standardnamen der Datei steht. Bei einer replacement-file ist das Erstellungsdatum identisch mit dem Erstellungsdatum der ersten Eingabedatei mit Standardnamen, aus der diese entstanden ist.

**DATE = \*INTERVAL(...)**

Das Erstellungsdatum im Standardnamen der Eingabedateien muss im angegebenen Intervall liegen. Die Jahreszahlangabe muss im Bereich 1960 bis 2059 liegen. Das Datum kann mit oder ohne Jahrhundert-Angabe definiert werden. Eine Jahreszahl ohne Jahrhundertangabe, die kleiner als 60 ist, wird diesem Jahrhundert zugerechnet, Jahreszahlangaben, die größer/gleich 60 sind, gelten für das vergangene Jahrhundert. Auch bei expliziter Angabe des Jahrhunderts müssen diese Grenzen eingehalten werden. Beispiel: Die Jahreszahl „1955“ ist deshalb nicht zulässig.

**FIRST-DATE = <date 8..10>**

Untere Grenze des Intervalls, in dem das Datum im Standardnamen der Eingabedateien liegen soll.

**LAST-DATE = <date 8..10>**

Obere Grenze des Intervalls, in dem das Datum im Standardnamen der Eingabedateien liegen soll.

**SESSION-NUMBER =**

Bestimmt, welche session-number die Eingabedateien haben sollen.

**SESSION-NUMBER = \*ALL**

Jede session-number im Standardnamen der Eingabedatei ist zugelassen.

**SESSION-NUMBER = <integer 1..999>**

Session-number, die im Standardnamen der Datei steht. Bei einer replacement-file ist die session-number identisch mit der session-number der ersten Eingabedatei mit Standardnamen, aus der diese entstanden ist.

**SESSION-NUMBER = \*RANGE(...)**

Die session-number im Standardnamen der Eingabedateien muss im angegebenen Bereich liegen.

**FIRST-SESSION-NUMBER = <integer 1..999>**

Untere Grenze des Bereichs, in dem die session-number im Standardnamen der Eingabedateien liegen soll.

**LAST-SESSION-NUMBER = <integer 1..999>**

Obere Grenze des Bereichs, in dem die session-number im Standardnamen der Eingabedateien liegen soll.

**SEQUENCE-NUMBER =**

Bestimmt, welche sequence-number die Eingabedateien haben sollen.

**SEQUENCE-NUMBER = \*ALL**

Jede sequence-number im Standardnamen der Eingabedatei ist zugelassen.

**SEQUENCE-NUMBER = <integer 1..999>**

Sequence-number, die im Standardnamen der Datei steht. Bei einer replacement-file ist die sequence-number identisch mit der sequence-number der ersten Eingabedatei mit Standardnamen, aus der diese entstanden ist.

**SEQUENCE-NUMBER = \*RANGE(...)**

Die sequence-number im Standardnamen der Eingabedateien muss im angegebenen Bereich liegen.

**FIRST-SEQU-NUMBER = <integer 1..999>**

Untere Grenze des Bereichs, in dem die sequence-number im Standardnamen der Eingabedateien liegen soll.

**LAST-SEQU-NUMBER = <integer 1..999>**

Obere Grenze des Bereichs, in dem die sequence-number im Standardnamen der Eingabedateien liegen soll.

**INPUT-FILES = list-poss(100): <filename 1..54>**

Dateiname der analysis-file, die als Eingabe für SATUT dient.



Hier können nur analysis-files angegeben werden. Dies sind Dateien, die in einem vorangegangenen SATUT-Lauf mit folgender Anweisung erzeugt wurden:

```
//SAVE-SELECTED-RECORDS ..., TO-REDUCTION-NAME=<filename 1..54>
```

SATLOG-Dateien, replacement-files und CONSLOG-Dateien müssen mit der Angabe INPUT-FILE=\*STD(...) als Eingabedateien vereinbart werden.

Für die Zuordnung der Datei SYS.SATLOG.2017-04-24.006.02 ist z.B. folgende INPUT-FILES-Angabe erforderlich:

```
INPUT-FILES=*STD( DATE=2017-04-24 , SESSION-NUMBER=6 , SEQUENCE-NUMBER=2 )
```

*Hinweise*

Um bei Eingabe von SATLOG-Dateien und/oder replacement-files und/oder CONSLOG-Dateien mögliche Überlappungen zu vermeiden, verfährt SATUT wie folgt:

1. Aus den Eingabedateien wird eine Liste mit den Protokolldateinamen erstellt:
  - ist die Eingabedatei eine SATLOG-Datei oder eine CONSLOG-Datei, wird ihr Name übernommen,
  - ist die Eingabedatei eine replacement-file, werden die Namen der SATLOG-Dateien / CONSLOG-Dateien übernommen, aus denen diese erzeugt wurde.
2. Erscheint der Name einer SATLOG-Datei / CONSLOG-Datei mehrmals in der nach 1. erzeugten Liste, wird die Anweisung zurückgewiesen.

*Beispiel*

Ein Benutzer mit dem Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION will die SATLOG-Dateien der Session 003 vom 02.05.2017 bis 09.05.2017 bearbeiten:

```
//select-input-files input-files=*std(type=*sat, subset=*std, -  
//      date=*interval(first-date=2017-05-02, last-date=2017-05-09), -  
//      session-number=003, sequence-number=*all)
```

oder in Kurzform:

```
//sel-inp-files *std(date=int(2017-05-02,2017-05-09),sess-num=003)
```

Als Ergebnis dieser Anweisung sucht der Auswerter unter SYSAUDIT die SATLOG-Dateien oder replacement-files, deren Erzeugungsdatum zwischen dem 02.05.2017 und dem 09.05.2017 liegt und deren session-number 003 ist.

## SELECT-RECORDS

### Aufbereitungsbedingung festlegen

Mit der Anweisung //SELECT-RECORDS werden eine Aufbereitungsbedingung festgelegt und die Datensätze ausgegeben, die diese Aufbereitungsbedingung erfüllen.

Die Auswahl der Datensätze mit //SELECT-RECORDS erfolgt stets aus den Eingabedateien in die Arbeitsdatei 0.

Während eines Auswertungslaufs kann immer nur eine Aufbereitungsbedingung gelten. Sollen für dieselben Eingabedateien noch andere Aufbereitungsbedingungen gelten, müssen diese in einem erneuten SATUT-Lauf mit SELECT-RECORDS festgelegt werden.

|                                                     |
|-----------------------------------------------------|
| <b>SELECT-RECORDS</b>                               |
| <b>CONDITION = *NONE / &lt;cmd-rest 0..1800&gt;</b> |

#### *Hinweis*

1. Diese Anweisung wird nur noch aus Kompatibilitätsgründen unterstützt.
2. Die Funktionalität von //SELECT-RECORDS wird von den Anweisungen //ADD-SELECTION-CONDITIONS und //START-SELECTION übernommen.

## SHOW-REDUCTION-FILES-ORIGIN

### Herkunft von replacement-files anzeigen

Mit der Anweisung //SHOW-REDUCTION-FILES-ORIGIN werden Informationen über die Ursprungsdateien von replacement-files ausgegeben.

| SHOW-REDUCTION-FILES-ORIGIN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> <b>PUBSET</b> = <b>*STD</b> / list-poss(20): &lt;cat-id 1..4&gt; <b>,DATE</b> = <b>*ALL</b> / &lt;date 8..10&gt; / <b>*INTERVAL</b>(...)   <b>*INTERVAL</b>(...)       <b>FIRST-DATE</b> = &lt;date 8..10&gt;       <b>,LAST-DATE</b> = &lt;date 8..10&gt; <b>,SESSION-NUMBER</b> = <b>*ALL</b> / &lt;integer 1..999&gt; / <b>*RANGE</b>(...)   <b>*RANGE</b>(...)       <b>FIRST-SESSION-NUMBER</b> = &lt;integer 1..999&gt;       <b>,LAST-SESSION-NUMBER</b> = &lt;integer 1..999&gt; <b>,SEQUENCE-NUMBER</b> = <b>*ALL</b> / &lt;integer 1..999&gt; / <b>*RANGE</b>(...)   <b>*RANGE</b>(...)       <b>FIRST-SEQU-NUMBER</b> = &lt;integer 1..999&gt;       <b>,LAST-SEQU-NUMBER</b> = &lt;integer 1..999&gt; <b>,OUTPUT</b> = <b>*SYSOUT</b> / <b>*SYSLST</b>(...)   <b>*SYSLST</b>(...)       <b>LINES-PER-PAGE</b> = <b>64</b> / &lt;integer 20..255&gt; </pre> |

#### **PUBSET =**

Gibt an, auf welchem Pubset die replacement-files zu finden sind.

Aus Kompatibilitätsgründen sind die Angaben PUBLIC-VOLUME-SET oder PUB-VOL-SET an Stelle von PUBSET noch zugelassen.

#### **PUBSET = \*STD**

SATUT sucht die replacement-files unter der Standard-Katalogkennung (DEFAULT-CATID) der Benutzerkennung SYSAUDIT.

#### **PUBSET = list-poss(20): <cat-id 1..4>**

SATUT sucht die replacement-files unter den angegebenen Katalogkennungen.

#### **DATE =**

Datum im Standard-Namen der replacement-files.

**DATE = \*ALL**

Jedes Datum ist für die Auswahl zulässig.

**DATE = <date 8..10>**

Erstellungsdatum der ersten Datei (SAT-Datei oder CONSLOG-Datei), aus der die replacement-files erzeugt wurden.

**DATE = \*INTERVAL(...)**

Das Datum im Standardnamen der replacement-files muss in einem Intervall liegen. Die Jahreszahlangabe muss im Bereich 1960 bis 2059 liegen. Das Datum kann mit oder ohne Jahrhundert-Angabe definiert werden. Eine Jahreszahl ohne Jahrhundertangabe, die kleiner als 60 ist, wird diesem Jahrhundert zugerechnet, Jahreszahlangaben, die größer/gleich 60 sind, gelten für das vergangene Jahrhundert. Auch bei expliziter Angabe des Jahrhunderts müssen diese Grenzen eingehalten werden. Beispiel: Die Jahreszahl „1955“ ist deshalb nicht zulässig.

**FIRST-DATE = <date 8..10>**

Untere Grenze des Intervalls, in dem das Datum liegen soll, welches im Standardnamen der replacement-files enthalten ist.

**LAST-DATE = <date 8..10>**

Obere Grenze des Intervalls, in dem das Datum liegen soll, welches im Standardnamen der replacement-files enthalten ist.

**SESSION-NUMBER =**

Session-number im Standard-Namen der replacement-files.

**SESSION-NUMBER = \*ALL**

Jede session-number ist für die Auswahl zulässig.

**SESSION-NUMBER = <integer 1..999>**

Session-number der ersten Datei (SAT-Datei oder CONSLOG-Datei), aus der die replacement-files erzeugt wurden.

**SESSION-NUMBER = \*RANGE(...)**

Die session-number im Standardnamen der replacement-files muss im angegebenen Bereich liegen.

**FIRST-SESSION-NUMBER = <integer 1..999>**

Untere Grenze des Bereichs, zu dem die session-number im Standardnamen der replacement-files gehören soll.

**LAST-SESSION-NUMBER = <integer 1..999>**

Obere Grenze des Bereichs, zu dem die session-number im Standardnamen der replacement-files gehören soll.

**SEQUENCE-NUMBER =**

Sequence-number im Standard-Namen der replacement-files.

**SEQUENCE-NUMBER = \*ALL**

Jede sequence-number ist für die Auswahl zulässig.

**SEQUENCE-NUMBER = <integer 1..999>**

Sequence-number der ersten Datei (SAT-Datei oder CONSLOG-Datei), aus der die replacement-files erzeugt wurden.

**SEQUENCE-NUMBER = \*RANGE(...)**

Die sequence-number im Standardnamen der replacement-files muss im angegebenen Bereich liegen.

**FIRST-SEQU-NUMBER = <integer 1..999>**

Untere Grenze des Bereichs, zu dem die sequence-number im Standardnamen der replacement-files gehören soll.

**LAST-SEQU-NUMBER = <integer 1..999>**

Obere Grenze des Bereichs, zu dem die sequence-number im Standardnamen der replacement-files gehören soll.

**OUTPUT = \*SYSOUT**

Die angeforderte Information soll auf SYSOUT ausgegeben werden.

**OUTPUT = \*SYSLST(...)**

Die angeforderte Information soll auf SYSLST ausgegeben werden.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

*Beispiel*

Der Ursprung der replacement-files mit Datum 4.5.2017 soll angezeigt werden:

```
//show-reduction-files-origin pubset=*std,date=2017-05-04, -
//                               output=sysout
```

oder in Kurzform:

```
//show-red-files-orig date=2017-05-04
```

*Ergebnis der Anweisung*

```
REDUCTION FILE NAME : :J:$SYSAUDIT.SYS.SATUT.2017-05-04.003.001
CREATION DATE:      2017-05-04-17.09.53.23
INPUT FILES:        SYS.SATLOG.2017-05-04.003.01
                    SYS.SATLOG.2017-05-04.003.02
SELECTION CONDITION : USER-ID IN-LIST('VALERIE','VALERE','MICHELE',
                    'ISABELLE','ARMAND','THIERRY','PHILIPPE') AND
                    FILNAME IN-LIST('SYS.SATUT.2017-05-01.001.001',
                    'SYS.SATUT.2017-05-01.001.002')
```

## SHOW-SELECTED-RECORDS

### Ausgewählte Datensätze ausdrucken

Mit der Anweisung //SHOW-SELECTED-RECORDS werden die Datensätze auf SYSLST oder in eine XML-Datei ausgegeben, die mit der Anweisung //START-SELECTION ausgewählt wurden.

Die Datensätze können entweder vollständig oder nur mit einem bestimmten Teil ihres Inhaltes ausgegeben werden.

Zur übersichtlicheren Ausgabe der Datensätze dient ein Sortierkriterium. Mit diesem können die Datensätze nach den stets vorhandenen Informationen sortiert werden.

#### SHOW-SELECTED-RECORDS

```

INFORMATION = *ALL-FIELDS / list-poss(100): <structured-name>
, SORT-CRITERION = *NONE / *USER-ID / *TSN / *EVT / *TIMESTP
, FROM-FILE = 0 / <integer 0..9>
, OUTPUT = *SYSLST(...)
  *SYSLST(...)
    | LINES-PER-PAGE = 64 / <integer 20..255>
, XML-OUTPUT = *NONE / *STD / <filename 1..38 without-cat-gen-user>

```

#### **INFORMATION =**

Bestimmt, welche Informationen aus den Datensätzen angezeigt werden.

Unabhängig davon, welche Werte bei INFORMATION angegeben werden, wird für alle Datensätze immer EVT und TIMESTP ausgegeben und - falls vorhanden - auch RES, TSN und USER-ID.

#### **INFORMATION = \*ALL-FIELDS**

Alle Datensätze werden vollständig angezeigt.

#### **INFORMATION = list-poss(100):<structured-name>**

Bestimmt die Feldnamen der Information aus den Datensätzen deren Inhalt ausgegeben werden soll (siehe „[Tabelle der protokollierbaren Informationen \(Feldnamen\)](#)“ auf [Seite 279ff](#)).

Da TIMESTP, TSN, USER-ID, RES und EVT für jeden Datensatz grundsätzlich ausgegeben werden, dürfen sie hier nicht angegeben werden.

**SORT-CRITERION =**

Bestimmt das Sortierkriterium für die Ausgabe der Datensätze.

Wird ein Sortierkriterium ungleich NONE gewählt, benötigt SAT zur Sortierung Arbeitsdateien.

**SORT-CRITERION = \*NONE**

Die Datensätze werden nicht nach speziellen Kriterien sortiert.

**SORT-CRITERION = \*TIMESTP**

Die Datensätze werden nach ihrem Zeit-Stempel sortiert.

**SORT-CRITERION = \*TSN**

Die Datensätze werden nach ihrer TSN und nach ihrem Zeit-Stempel sortiert.

**SORT-CRITERION = \*USER-ID**

Die Datensätze werden nach Benutzerkennungen und nach ihrem Zeit-Stempel sortiert.

**SORT-CRITERION = \*EVT**

Die Datensätze werden nach Ereignis-Typen und nach ihrem Zeit-Stempel sortiert.

**FROM-FILE = 0 / <integer 0..9>**

Arbeitsdatei, deren Inhalt ausgegeben wird.

**OUTPUT = \*SYSLST(...)**

Die Information wird auf SYSLST ausgegeben.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

**XML-OUTPUT =**

Gibt an, ob die Information in eine XML-Datei ausgegeben werden soll.

**XML-OUTPUT = \*NONE**

Es wird keine XML-Datei erzeugt.

**XML-OUTPUT = \*STD**

Die Information wird im XML-Format in eine Datei ausgegeben. Diese Datei wird mit dem Standard-Namen \$SYSAUDIT.SYS.SATUT.yyyy-mm-dd.sss.nnn.XML angelegt, wobei:

yyyy-mm-dd      Erstellungsdatum der (zeitlich) ersten Datei der Eingabedateien, aus denen die XML-Datei erzeugt wurde

sss                session-number

nnn                Folgenummer der Datei in der Session (1..999)

**XML-OUTPUT = <filename 1..38 without-cat-gen-user>**

Die Information wird im XML-Format in eine Datei mit dem angegebenen Namen ausgegeben.

Falls die Datei bereits existiert, erhält der Benutzer im Dialog-Betrieb eine Abfrage, ob er die Datei überschreiben möchte, in einem Batch-Job wird das Kommando abgewiesen und eine entsprechende Meldung ausgegeben.

*Hinweise*

1. Die Inhalte der Arbeitsdateien (0 bis 9) werden mit dieser Anweisung nicht geändert.
2. Die Einträge in CONSLOG-Dateien werden vor der Ausgabe in entsprechende SATLOG-Sätze vom Typ CLG bzw. SKP umgewandelt.
3. Die Felder FILPOS, CURLIM2 und MAXLIM2 werden immer in der Einheit 512B (= Vielfache von 512 Byte) ausgegeben.



Die Ausgabe zum Ereignis UAD („Userid hinzufügen“) enthält eine Parameterliste, in diesem Fall die des Kommandos ADD-USER. Die Zeichenfolge „\*SECRET“ in dieser Ausgabe wird von SATCP im SATLOG-Satz an Stelle des Kennworts eingetragen, das in dieser Parameterliste enthalten ist.

### **Auswertungshinweise für \*LNG-Felder in SATLOG-Sätzen**

Um ein unberechtigtes Eindringen in den Rechenzentrumsbetrieb noch besser erkennen zu können, wird bei einigen Ereignissen zusätzlich der Inhalt der Parameterliste aufgezeichnet, über die das Ereignis ausgelöst wurde. Die Aufzeichnung erfolgt nur, wenn für die Preselection in SATCP der Operand LOGGING-QUANTITY=\*EXTENDED angegeben wurde. Da Parameterlisten i.A. länger als 255 Byte sein können, werden sie in Form von \*LNG-Feldern aufgezeichnet (siehe [Abschnitt „Aufbau der SATLOG-Dateien“ auf Seite 51](#)).

\*LNG-Felder werden hexadezimal und zeichenweise durch SATUT aufbereitet. Für die Auswertung der Parameterliste müssen i.A. die entsprechenden Schnittstellen-Makros (MF=D) herangezogen werden. SATUT liefert in der jeweiligen Feldbeschreibung einen kurzen Hinweis, wonach der Inhalt der Parameterliste ausgewertet werden kann.

Ist ein Makro für eine Schnittstellenbeschreibung angegeben, so befindet sich das Makro normalerweise in der Bibliothek \$TSOS.MACROLIB.

Überschreitet der Inhalt einer Parameterliste die Kapazität eines SATLOG-Satzes, so wird die Parameterliste über mehrere SATLOG-Sätze verteilt. Alle Teilsätze eines solchen SATLOG-Satzes enthalten in ihrem festen Teil die gleichen Informationen, so ist die Auswertung jedes Teilsatzes durch SATUT möglich.

Infolge asynchroner Verarbeitung in SATCP, ist die Reihenfolge der Teilsätze in der SATLOG-Datei nicht garantiert. Bei der Auswertung durch SATUT ist ggf. eine Sortierung notwendig. SATUT zeigt in der Feldbeschreibung an, welcher Teil des Feldes aufgelistet wird. Das letzte Teilstück eines SATLOG-Satzes ist durch die Zeichenfolge „LAST“ (letztes) an Stelle von einer Nummer gekennzeichnet. Zusätzlich wird die Distanz zum Anfang der Parameterliste ausgegeben.

#### *Beispiel*

Die folgende Ausgabe enthält eine Parameterliste, die auf zwei SATLOG-Teilsätze verteilt wurde. Im ersten Teilsatz (LOG\_REC\_PART = 1) werden die ersten 928 Byte der Parameterliste angezeigt (Distanz 0000 bis 039F) und im zweiten und letzten Teil die restlichen 342 Byte (Distanz 03A0 bis 04F5).



## SHOW-SELECTION-CONDITIONS

### Auswahlbedingungen anzeigen

Mit der Anweisung SHOW-SELECTION-CONDITIONS werden Informationen über die Auswahlbedingungen auf SYSOUT oder SYSLST angezeigt.

|                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SHOW-SELECTION-CONDITIONS</b>                                                                                                                                                   |
| <b>NAME</b> = <u>*ALL</u> / list-poss(10): <name 1..8><br><b>OUTPUT</b> = <u>*SYSOUT</u> / *SYSLST(...)<br>*SYSLST(...)<br>  <b>LINES-PER-PAGE</b> = <u>64</u> / <integer 20..255> |

**NAME** = \*ALL / list-poss(10): <name 1..8>  
Name der Auswahlbedingungen.

**NAME** = \*ALL  
Alle Auswahlbedingungen sollen ausgegeben werden.

**NAME** = list-poss(10): <name 1..8>  
Name der Auswahlbedingung, deren Wert ausgegeben werden soll.

**OUTPUT** = \*SYSOUT / \*SYSLST(...)  
Gibt an, wohin die angeforderte Information ausgegeben werden soll.

**OUTPUT** = \*SYSOUT  
Die angeforderte Information soll auf SYSOUT ausgegeben werden.

**OUTPUT** = \*SYSLST(...)  
Die angeforderte Information soll auf SYSLST ausgegeben werden.

**LINES-PER-PAGE** = 64 / <integer 20..255>  
Bestimmt das Ausgabeformat. Standard-Wert ist 64.

#### Beispiel

Der Wert der Bedingung COND1 soll ausgegeben werden:

```
//show-selection-conditions name=cond1
```

#### Ergebnis der Anweisung

```
SELECTION CONDITION NAME : COND1
SELECTION CONDITION      :
                          EVT EQUAL 'FRD'
```

## SHOW-STATISTICS

### SAT-Statistiken ausgeben

Mit der Anweisung //SHOW-STATISTICS werden ausgewählte Datensätze in einer Statistik angezeigt. Dies sind ausgewählte Datensätze aus den SATUT-Eingabedateien oder mit //START-SELECTION ausgewählte und aufbereitete Datensätze.

In Abhängigkeit von der gewählten Eingabe wird die zur Verfügung stehende Information interpretiert. SAT betrachtet alle durch die Eingabe zur Verfügung gestellten Daten als einer Sitzung zugehörig. Die Werte für „begin of analyzed period“ und „end of analyzed period“ werden aus dem ersten Eintrag der ersten Datei und dem letzten Eintrag der letzten Datei gewonnen.

„Elapsed time“ repräsentiert die Differenz dieser beiden Daten. Liegen diese beiden Daten sehr weit auseinander und enthalten die Daten aus der Eingabe große Lücken kann die Auswertung zu unerwarteten Ergebnissen führen. Jede Auswertung von SAT ist in Hinsicht auf die ausgewählten Daten zu interpretieren.

Die Daten geben Auskunft über:

1. Globale SAT-Daten
2. eine Zusammenfassung aller Ereignisse in Ereignisklassen
3. vollständige SAT-Statistik für jeden Ereignis-Typ
4. Optional kann ein Histogramm über die Anzahl Ereignisse pro Minute auf SYSLST ausgegeben werden.

#### SHOW-STATISTICS

```

MACHINE-SPEED = *UNDEFINED / <fixed 0.01..500>
,FROM-FILE = 0 / <integer 0..9> / *INPUT-FILES
,HISTOGRAM = *NO / *YES
,OUTPUT = *SYSLST(...) / SYSOUT
  *SYSLST(...)
    | LINES-PER-PAGE = 64 / <integer 20..255>

```

#### **MACHINE-SPEED = \*UNDEFINED / <fixed 0.01..500>**

Geschwindigkeit des Rechners in RPF. Dieser Parameter wird verwendet, um die Anzahl der Datensätze pro RPF und Stunde in den SAT-Statistiken auszurechnen.

Wenn für diesen Operanden kein Wert angegeben wird, entfallen bei der Ausgabe der Statistiken

- die Zeile "Machine speed" in den globalen SAT-Daten  
und
- die Spalte "# events/Mips/h" in der Zusammenfassung aller Ereignisse.

**FROM-FILE = 0 / <integer 0..9> / \*INPUT-FILES**

Datei, aus der die Statistik erstellt wird.

**FROM-FILE = 0 / <integer 0..9>**

Die Statistik wird aus der Arbeitsdatei mit der angegebenen Nummer erstellt.

**FROM-FILE = \*INPUT-FILES**

Die Statistik wird aus den Eingabedateien von SATUT erstellt (/SELECT-INPUT-FILES).

**HISTOGRAM =**

Bestimmt, ob ein Histogramm ausgegeben werden soll oder nicht. Ein Histogramm wird nur bei OUTPUT=\*SYSLST ausgegeben.

**HISTOGRAM = \*NO**

Es wird kein Histogramm erstellt und ausgegeben.

**HISTOGRAM = \*YES**

Es wird ein Histogramm erstellt und ausgegeben.

**OUTPUT = \*SYSLST(...) / \*SYSOUT**

Gibt an, wohin die angeforderte Information ausgegeben werden soll.

**OUTPUT = \*SYSLST(...)**

Die angeforderte Information wird auf SYSLST ausgegeben.

**LINES-PER-PAGE = 64 / <integer 20..255>**

Bestimmt die Zeilenzahl der Ausgabeseite.

**OUTPUT = \*SYSOUT**

Die angeforderte Information wird auf SYSOUT ausgegeben.

*Hinweise*

1. Diese Anweisung wertet alle angegebenen Dateien zeitlich sequenziell aus. Wurde die SAT-Protokollierung zwischenzeitlich ausgeschaltet, oder traten, z.B. wegen geringer Systemauslastung, eine Zeitlang keine Ereignisse auf, dann hat das folgende Auswirkungen. SATUT gibt für die ersten vier Minuten eines „ereignislosen“ Zeitraums Histogrammzeilen mit Nullwerten aus. Damit in der Liste nicht unnötig viele Leerzeilen enthalten sind, unterdrückt SATUT ab der 5. Minute des „ereignislosen“ Zeitraums die

Ausgabe von leeren Histogrammzeilen bis zum Auftreten des nächsten Ereignisses. Der Zeitraum, in dem die Ausgabe unterbrochen war, wird durch eine Zeile mit folgendem Inhalt dargestellt:

```
*** ----- No events for          n minutes ----- ***
```

Dabei ist n die Anzahl der Minuten, in denen die Ausgabe unterdrückt war.

### Beispiel

Ausschnitt eines Histogramms mit Zeiträumen, in denen keine Ereignisse auftraten

```
2017/04/02 12:20      741 | FFFFFFFF| FFFFFFFF| LLLLLLLLL| LLLLLSXXX| XXXX
2017/04/02 12:21      623 | FFFFFFFF| FFFFFFFF| FFFFFFFF| FFFFFFFLSX
2017/04/02 12:22      217 | FFFFFFFF| FFF
2017/04/02 12:23        0 |
2017/04/02 12:24        0 |
2017/04/02 12:25        0 |
2017/04/02 12:26        0 |
*** ----- No events for          2 minutes ----- ***
2017/04/02 12:29        7 | BJSX
2017/04/02 12:30        0 |
2017/04/02 12:31       18 | BFJLUX
2017/04/02 12:32        0 |
2017/04/02 12:33        7 | BFJ
2017/04/02 12:34        0 |
2017/04/02 12:35        0 |
2017/04/02 12:36        0 |
2017/04/02 12:37        0 |
*** ----- No events for          25 minutes ----- ***
2017/04/02 13:03        4 | SX
```

In diesem Beispiel gibt es zwei Zeiträume ohne protokollierte Ereignisse (von 12:23 bis 12:28 und von 12:34 bis 13:02). Die ersten vier Minuten dieser Zeiträume werden jeweils durch Histogrammzeilen mit Nullwerten dargestellt, die restliche Zeit durch Ausgabe einer Zeile, die ihre Länge in Minuten angibt.

2. Die Inhalte der Arbeitsdateien (0 bis 9) werden mit dieser Anweisung nicht geändert.
3. Wenn die CONSLOG-Dateien nicht das gleiche Format wie die SAT-Dateien haben, müssen sie konvertiert werden, um sie in einer Statistik auszugeben. Wenn die Dateien, die in einer Statistik ausgegeben werden sollen, noch nicht aufbereitet wurden, wird die Meldung SAE5152 ausgegeben und die Anweisung wird abgebrochen.

## Ausgabe der Statistiken

Das Ergebnis der Anweisung //SHOW-STATISTICS wird auf SYSLST oder SYSOUT ausgegeben. Die Ausgabe besteht aus mehreren Tabellen, die im Folgenden erklärt werden.

### 1. Globale SAT-Daten

- Datum und Uhrzeit des Auswertungslaufs
- Namen der Eingabedateien oder Name der bei //SELECT-RECORDS bzw. //START-SELECTION angegebenen Dateien
- Beginn und Ende der ausgewerteten Periode  
Anfangszeit und -datum des SATUT-Laufs werden dem Zeitstempel des ersten Datensatzes der ältesten SAT-Datei entnommen. Endzeit und -datum werden dem Zeitstempel des letzten Datensatzes der jüngsten SAT-Datei entnommen.
- Elapsed time: Differenz zwischen Anfangs- und Endzeit in Sekunden
- Machine speed: Rechnerleistung in MIPS, falls der Operand MACHINE-SPEED angegeben wurde
- Records/hour: Durchschnittliche Anzahl von Datensätzen, die pro Stunde in die SAT-Datei(en) protokolliert wurden
- # of records: Summe aller Protokolldatensätze der SAT-Eingabedatei(en) oder Anzahl durch //SELECT-RECORDS bzw. //START-SELECTION ausgewählter Datensätze.
- Mean length: Durchschnittliche Länge der Protokolldatensätze, errechnet aus allen ausgewählten Protokolldatensätzen der SAT-Eingabedateien.
- Mean kbytes/hour: Durchschnittliche Bytezahl, die pro Stunde in die SAT-Eingabedatei(en) geschrieben wurde. Diese Angabe ist nicht aussagekräftig, wenn nur einzelne Datensätze mit //SELECT-RECORDS bzw. //START-SELECTION ausgewählt wurden.

#### Beispiel

```
//show-statistics output=*sysout
Input-files of statement = :PC04:$SYSAUDIT.SYS.SATLOG.2017-04-01.137.01
                        :PC04:$SYSAUDIT.SYS.SATLOG.2017-04-01.137.02
                        :PC04:$SYSAUDIT.SYS.SATLOG.2017-04-02.137.03

Begin of analyzed period : 2017/04/01 10:19:21.24
End   of analyzed period : 2017/04/02 17:44:34.23
Elapsed time              =      113113 s      = 1 d 26713 s
Records/hour              =          53.56
# of records              =          1683
Mean length               =         102.00
Mean kbytes/hour         =           5.54
```

## 2. Zusammenfassung aller Ereignisse

In dieser Statistik werden alle Ereignisse in Ereignis-Klassen zusammengefasst.

Es wird jeweils die Gesamtmenge der aufgetretenen Ereignisse in der jeweiligen Ereignis-Klasse errechnet (# events), sowie die durchschnittliche Anzahl dieser Ereignisse pro Stunde (# events/h) und, falls der Operand MACHINE-SPEED angegeben wurde, die durchschnittliche Anzahl dieser Ereignisse pro MIPS pro Stunde (# events/ Mips/h).

Folgende Ereignis-Klassen werden statistisch erfasst:

1. DMS
  - Files (Dateizugriffe)
  - Security (Zugriff auf Schutzattribute im Benutzerkatalog)
  - Rename Files (Umbenennen von Dateien)
2. Catalog Management  
(Importieren und exportieren von Pubsets)
3. Job Enable (Dialog & Batch)  
(LOGON für Dialog und Batchauftrag im Erfolgs- und Fehlerfall)
4. Job (Rest)  
(Job-Ereignisse ohne LOGON für Dialog und Batchauftrag)
5. Job Variables  
(JVs: Zugriffe auf JVs)
6. BLS  
(Binder und Lader System: Laden und entladen von (Teilen von) TU-Programmen)
7. Spool
  - Jobs (Kommandos)
  - Devices (Verwaltung)
8. PLAM/ILAM  
(Zugriff auf Bibliothekselemente)
9. DSSM (Dynamic Subsystem Management)
  - Connection/Disconnection  
(TU-Aufträge einem nicht privilegierten Subsystem zuweisen/entziehen)
  - Catalog Management  
(DSSM Katalogverwaltung)
10. Syntax Files  
(Zugriff auf Syntaxdateien)

- 11. Users/Groups/Privileges
  - Users (Verwaltung von Benutzerkennungen)
  - Privileges (Verwaltung von Privilegien)
  - Groups (Verwaltung von Benutzergruppen)
- 12. Object Protection
  - GUARDS (Standard-Bedingungsverwaltung)
  - Coowner Protection (Miteigentümerschutz)
  - Default Protection (Standardschutz)
  - Access Control List (ACL: Zugriff auf ACL-Einträge)
- 13. System Access Control Management
  - Terminal Sets (Verwaltung von Terminal Sets)
  - Operator Roles (Verwaltung von Operator Roles)
  - Keys (Objekt KEY)
- 14. SAT (SAT-Ereignisse)
- 15. UTM (UTM-Ereignisse)
- 16. SESAM (SESAM-Ereignisse)
- 17. POSIX
  - Files and Directories
  - Child Processes
  - Processes
  - System Resources (Ereignisse der entsprechenden Objekte)
- 18. Communication Methods
  - DCAM
  - BCAM
  - IP Security (Ereignisse der entsprechenden Objekte)
- 19. Memory Pools (eröffnen, schließen, freigeben, zugreifen)

20. Events
  - Serialization
  - Eventing
  - (ein- und ausschalten von Ereignissteuerung und Serialisierung)
21. Fast Intertask Communication  
(Objekt FITC)
22. Storage Class Events  
(Objekt SMS)
23. Data Spaces
24. Volume  
(Bänder mit MAREN bearbeiten und verwalten; Datenträger mit NDM bearbeiten;  
Datenträger mit FDDRL, VOLIN oder IOCFCOPY bearbeiten)
25. ADAM Device Management
26. ANY event (system exit)

*Beispiel*

## SUMMARY OF EVENTS

| Event class                           | # events | # events/h | # events/Mips/h |
|---------------------------------------|----------|------------|-----------------|
| 1 : DMS                               |          |            |                 |
| Files                                 | 711      | 22.63      | 4.53            |
| Security                              | 733      | 23.33      | 4.67            |
| Rename Files                          | 5        | 0.16       | 0.03            |
| 2 : Catalog Management                | 0        | 0.00       | 0.00            |
| 3 : Job Enable (Dialog & Batch)       |          |            |                 |
| Success                               | 33       | 1.05       | 0.21            |
| Failure                               | 6        | 0.19       | 0.04            |
| 4 : Job (Rest)                        | 33       | 1.05       | 0.21            |
| 5 : Job Variables                     | 0        | 0.00       | 0.00            |
| 6 : BLS                               | 15       | 0.48       | 0.10            |
| 7 : Spool                             |          |            |                 |
| Jobs                                  | 0        | 0.00       | 0.00            |
| Devices                               | 0        | 0.00       | 0.00            |
| 8 : PLAM/ILAM                         | 20       | 0.64       | 0.13            |
| 9 : DSSM                              |          |            |                 |
| Connection/Disconnection              | 2        | 0.06       | 0.01            |
| Catalog Management                    | 17       | 0.54       | 0.11            |
| 10 : Syntax Files                     | 0        | 0.00       | 0.00            |
| 11 : Users/Groups/Privileges          |          |            |                 |
| Users                                 | 87       | 2.77       | 0.55            |
| Privileges                            | 0        | 0.00       | 0.00            |
| Groups                                | 0        | 0.00       | 0.00            |
| 12 : Object Protection                |          |            |                 |
| GUARDS                                | 0        | 0.00       | 0.00            |
| Coowner Protection                    | 0        | 0.00       | 0.00            |
| Default Protection                    | 0        | 0.00       | 0.00            |
| Access Control List                   | 0        | 0.00       | 0.00            |
| 13 : System Access Control Management |          |            |                 |
| Terminal Sets                         | 0        | 0.00       | 0.00            |
| Operator Roles                        | 0        | 0.00       | 0.00            |
| Keys                                  | 13       | 0.41       | 0.08            |
| 14 : SAT                              | 2        | 0.06       | 0.01            |
| 15 : UTM                              | 0        | 0.00       | 0.00            |
| 16 : SESAM                            | 0        | 0.00       | 0.00            |
| 17 : POSIX                            |          |            |                 |
| Files and Directories                 | 0        | 0.00       | 0.00            |
| Child Processes                       | 0        | 0.00       | 0.00            |
| Processes                             | 0        | 0.00       | 0.00            |
| System Resources                      | 0        | 0.00       | 0.00            |
| 18 : Communication Methods            |          |            |                 |
| DCAM                                  | 0        | 0.00       | 0.00            |
| BCAM                                  | 0        | 0.00       | 0.00            |
| IP Security                           | 0        | 0.00       | 0.00            |
| 19 : Memory Pools                     | 0        | 0.00       | 0.00            |
| 20 : Events                           |          |            |                 |
| Serialization                         | 0        | 0.00       | 0.00            |
| Eventing                              | 0        | 0.00       | 0.00            |
| 21 : Fast Intertask Communication     | 0        | 0.00       | 0.00            |
| 22 : Storage Class Events             | 0        | 0.00       | 0.00            |
| 23 : Data Spaces                      | 0        | 0.00       | 0.00            |
| 24 : Volume                           | 0        | 0.00       | 0.00            |
| 25 : ADAM device management           | 0        | 0.00       | 0.00            |
| 26 : ANY event (system exit)          | 0        | 0.00       | 0.00            |

### 3. Vollständige SAT-Statistik für jeden Ereignis-Typ

Die Statistik für jedes Einzel-Ereignis wird in alphabetischer Reihenfolge nach den Kurznamen aufgelistet (Kurznamen siehe [Abschnitt „Tabelle der Objektereignisse“ auf Seite 196](#)).

Für jedes Ereignis werden folgende Informationen erstellt:

|                |                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EVENT          | Ereignis-Kurzname                                                                                                                                                                                                                      |
| # SUCC         | Anzahl der Protokoll-Datensätze mit Ergebnis SUCCESS, die für dieses Ereignis protokolliert wurden                                                                                                                                     |
| # FAIL         | Anzahl der Protokoll-Datensätze mit Ergebnis FAILURE, die für dieses Ereignis protokolliert wurden                                                                                                                                     |
| # NONE         | Zahl sollte 0 sein; ist das nicht der Fall, stellen Sie fest, ob diese Protokoll-Datensätze nicht von einer Exit-Routine des Rechenzentrums stammen (Ereignis-Typ ANY); falls das nicht zutrifft, verständigen Sie bitte die Wartung). |
| LEN SUCC       | Durchschnittliche Länge der Protokolldatensätze für diesen Ereignis-Typ mit Ergebnis SUCCESS                                                                                                                                           |
| LEN FAIL       | Durchschnittliche Länge der Protokolldatensätze für diesen Ereignis-Typ mit Ergebnis FAILURE                                                                                                                                           |
| LEN NONE       | Durchschnittliche Länge der Protokolldatensätze für diesen Ereignis-Typ ohne Ergebnis                                                                                                                                                  |
| % EVENTS       | Verhältnis (in Prozent) zwischen der Summe von # SUCC, # FAIL und # NONE und der Menge aller auszuwertenden Protokolldatensätze.                                                                                                       |
| % FAIL (EVENT) | Verhältnis (in Prozent) zwischen der Summe der Protokolldatensätze dieses Ereignis-Typs mit Ergebnis FAILURE und der Summe aller Protokoll-Datensätze mit Ergebnis SUCCESS, FAILURE und NONE.                                          |
| RECORDS/HOUR   | Durchschnittliche Menge von Protokolldatensätzen für diesen Ereignis-Typ, die in einer Stunde protokolliert wird                                                                                                                       |

In dieser Statistik werden nur solche Ereignis-Typen aufgelistet, die in den Eingabedateien für SHOW-STATISTICS vorhanden sind.

Bei Ausgabe auf SYSOUT werden die Werte # NONE, LEN SUCC, LEN FAIL und LEN NONE unterdrückt.

*Beispiel*

| #      | EVENT | # SUCC | # FAIL | # NONE | LEN SUCC | LEN FAIL | LEN NONE | % EVENTS | % FAIL(EVENT) | RECORDS/HOUR |
|--------|-------|--------|--------|--------|----------|----------|----------|----------|---------------|--------------|
| 1      | FCD   | 59     | 0      | 0      | 108.61   | 0.00     | 0.00     | 3.51     | 0.00          | 1.88         |
| 2      | FCL   | 298    | 0      | 0      | 97.52    | 0.00     | 0.00     | 17.71    | 0.00          | 9.48         |
| 3      | FCS   | 58     | 0      | 0      | 106.02   | 0.00     | 0.00     | 3.45     | 0.00          | 1.85         |
| 4      | FDD   | 64     | 2      | 0      | 100.62   | 99.00    | 0.00     | 3.92     | 3.03          | 2.10         |
| 5      | FDS   | 64     | 20     | 0      | 103.94   | 100.50   | 0.00     | 4.99     | 23.81         | 2.67         |
| 6      | FED   | 33     | 0      | 0      | 101.09   | 0.00     | 0.00     | 1.96     | 0.00          | 1.05         |
| 7      | FMD   | 92     | 0      | 0      | 95.16    | 0.00     | 0.00     | 5.47     | 0.00          | 2.93         |
| 8      | FMS   | 11     | 0      | 0      | 121.91   | 0.00     | 0.00     | 0.65     | 0.00          | 0.35         |
| 9      | FRD   | 162    | 1      | 0      | 100.68   | 97.00    | 0.00     | 9.69     | 0.61          | 5.19         |
| 10     | FRN   | 5      | 0      | 0      | 148.60   | 0.00     | 0.00     | 0.30     | 0.00          | 0.16         |
| 11     | FRS   | 391    | 189    | 0      | 106.45   | 110.13   | 0.00     | 34.46    | 32.59         | 18.46        |
| 12     | JBE   | 16     | 2      | 0      | 81.06    | 71.50    | 0.00     | 1.07     | 11.11         | 0.57         |
| 13     | JDE   | 17     | 4      | 0      | 79.29    | 83.75    | 0.00     | 1.25     | 19.05         | 0.67         |
| 14     | JED   | 16     | 0      | 0      | 58.94    | 0.00     | 0.00     | 0.95     | 0.00          | 0.51         |
| 15     | JIN   | 17     | 0      | 0      | 69.00    | 0.00     | 0.00     | 1.01     | 0.00          | 0.54         |
| 16     | KTC   | 13     | 0      | 0      | 125.00   | 0.00     | 0.00     | 0.77     | 0.00          | 0.41         |
| 17     | LCL   | 10     | 0      | 0      | 128.50   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 18     | LEE   | 10     | 0      | 0      | 124.50   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 19     | SCR   | 14     | 3      | 0      | 79.71    | 78.33    | 0.00     | 1.01     | 17.65         | 0.54         |
| 20     | SDS   | 2      | 0      | 0      | 85.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 21     | UAD   | 2      | 0      | 0      | 81.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 22     | UCK   | 71     | 10     | 0      | 82.70    | 82.90    | 0.00     | 4.81     | 12.35         | 2.58         |
| 23     | UML   | 2      | 0      | 0      | 81.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 24     | URM   | 1      | 1      | 0      | 81.00    | 81.00    | 0.00     | 0.12     | 50.00         | 0.06         |
| 25     | XLD   | 10     | 0      | 0      | 199.00   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 26     | XUL   | 5      | 0      | 0      | 80.00    | 0.00     | 0.00     | 0.30     | 0.00          | 0.16         |
| 27     | ZBG   | 3      | 0      | 0      | 245.33   | 0.00     | 0.00     | 0.18     | 0.00          | 0.10         |
| 28     | ZCH   | 2      | 0      | 0      | 130.00   | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 29     | ZND   | 3      | 0      | 0      | 83.33    | 0.00     | 0.00     | 0.18     | 0.00          | 0.10         |
| TOTAL: |       | 1451   | 232    | 0      | 101.26   | 106.65   | 0.00     | 100.00   | 13.78         | 53.6         |

#### 4. Optional: Histogramm der Ereignisse pro Minute

Für jede Minute des protokollierten Zeitraums wird ein Histogramm erstellt, das die Anzahl und die Art von Ereignissen anzeigt.

Die Achse, auf der die Ereignisquantität dargestellt wird, ist in Prozentschritte unterteilt. Jede Stufe stellt 10% dar, jeder Buchstabe 1% der maximal möglichen Anzahl von Ereignissen pro Minute. Jede Minute, in der dieses Maximum erreicht wurde, wird im Histogramm mit einem '\*' versehen.

Jede Zeile des Histogramms enthält folgende Information (von links nach rechts):

- Datum
- Uhrzeit
- Anzahl der Ereignisse in dieser Minute
- '\*' wenn die maximal mögliche Anzahl von Ereignissen pro Minute protokolliert wurde
- die Histogrammzeile mit der Verteilung der Ereignisse pro Ereignisart

*Beispiel (auf SYSLST)*

```
/show-statistics from-file=*input-files, -  
/                histogram=*yes, output=*syslst
```

*Hinweis*

Wenn in der Folge der angegebenen SAT-Dateien oder in der Zeitspanne, die von den Eingabedateien abgedeckt wird, Lücken vorhanden sind, werden diese wie Zeiträume behandelt, in denen keine Ereignisse aufgetreten sind. In den ersten vier Minuten einer solchen Lücke enthält das Histogramm Zeilen, bei denen die Menge der Ereignisse pro Minute gleich Null ist, ab der fünften Minute wird eine Zeile ausgegeben, die angibt, wie lange keine Ereignisse aufgetreten sind.

SATUT V05.5A 2017-04-06 16:17:07 PAGE 4

PROCESSED STATEMENT : SHOW-STATISTICS

```
*****
# +-----+-----+-----+-----+-----+-----+-----+-----+
2017/04/01 10:19 1 |ZZ
2017/04/01 10:20 37 |FFFFFFFF|FFFFFFFJ|JJJJJKSS|SSSSSSSS|SUUUU
2017/04/01 10:21 35 |FFFFFFFF|FFFFFFFJ|FFFJJJJJ|JJSSSSUU|UU
2017/04/01 10:22 4 |JJKUUU
2017/04/01 10:23 1 |UU
2017/04/01 10:24 4 |JJKUUU
2017/04/01 10:25 2 |JJUU
2017/04/01 10:26 3 |JJUU
2017/04/01 10:27 2 |JJUU
2017/04/01 10:28 0 |
2017/04/01 10:29 0 |
2017/04/01 10:30 0 |
2017/04/01 10:31 3 |FFFUU
2017/04/01 10:32 1 |UU
...
2017/04/02 16:48 30 |FFFFFFFF|FFFFFFFJ|FFFFFFFJ|FFFX
2017/04/02 17:27 2 |FFF
2017/04/02 17:28 22 |FFFFFFFF|FFFFFFFJ|LLLLXX
2017/04/02 17:42 5 |FFFFFJJ
2017/04/02 17:43 19 |FFFFFFFF|FFFFFFJJ|SSXX
2017/04/02 17:44 2 |FFZZ
# +-----+-----+-----+-----+-----+-----+-----+-----+

```

SATUT V05.5A 2017-04-06 16:17:07 PAGE 9

PROCESSED STATEMENT : SHOW-STATISTICS

\*\*\*\*\*

EXPLANATION ON USED LETTERS:

- F : FCD, FCL, FCS, FDD, FDS, FED, FMD, FMS, FRD, FRN, FRS
- J : JBE, JDE, JED, JIN
- K : KTC
- L : LCL, LEE
- S : SCR, SDS
- U : UAD, UCK, UML, URM
- X : XLD, XUL
- Z : ZBG, ZCH, ZND

## START-SELECTION

### Auswertung einleiten

Mit der Anweisung //START-SELECTION werden Datensätze ausgewählt, die der vorgegebenen Auswahlbedingung genügen. Die aufbereiteten Datensätze werden für jede Auswahlbedingung in eine eigene Arbeitsdatei abgelegt, die durch eine Nummer gekennzeichnet ist.

Dies geschieht in einem Schritt, d.h. jede Eingabedatei wird nur einmal gelesen.

Als Ergebnis der Anweisung wird die Anzahl der aufbereiteten Datensätze je Arbeitsdatei ausgegeben.

#### START-SELECTION

**FROM-FILE = q / <integer 0..9> / \*INPUT-FILES**

, **TO-FILE = list-poss(10): \*PARAMETERS(...)**

**\*PARAMETERS(...)**

**FILE = q / <integer 0..9>**

**,CONDITION-NAME = <name 1..8>**

#### **FROM-FILE = q / <integer 0..9> / \*INPUT-FILES**

Quelle der Datensätze.

#### **FROM-FILE = q / <integer 0..9>**

Die Datensätze werden aus der Arbeitsdatei mit der angegebenen Nummer ausgewählt.

#### **FROM-FILE = \*INPUT-FILES**

Die Datensätze werden aus den Eingabedateien von SATUT ausgewählt, die in der Anweisung SELECT-INPUT-FILES ausgewählt wurden.

#### **TO-FILE = \*PARAMETERS(...)**

Bestimmt die Bedingung und das Ausgabeziel der Aufbereitung.

#### **FILE = q / <integer 0..9>**

Angabe der Arbeitsdatei, in die die ausgewählten Datensätze geschrieben werden.

#### **CONDITION-NAME = <name 1..8>**

Name der Auswahlbedingung, die in der Anweisung //ADD-SELECTION-CONDITIONS bestimmt wurde.

*Hinweise*

1. Wurde eine Arbeitsdatei, die als Ausgabe im Operanden TO-FILE bestimmt wird, bereits in einem SATUT-Lauf verwendet, so wird diese überschrieben.
2. Wird in den Operanden FROM-FILE und TO-FILE die gleiche Datei angegeben, wird die Arbeitsdatei überschrieben.

*Beispiel*

Datensätze aus den Eingabedateien werden nach der Auswahlbedingung COND1 ausgewählt und in der Arbeitsdatei 3 abgelegt.

```
//start-selection from-file=*input-files, -  
//                to-file=*parameters(file=3,condition=cond1)
```

Als Ergebnis der Anweisung wird die Anzahl der aufbereiteten Datensätze ausgegeben:

```
SAE7001: START-SELECTION TERMINATED.'123' RECORDS SELECTED IN WORK  
FILE'3'
```

## 2.6.7 Auswertungsbeispiel

Beispiele für die Bildung komplexer Bedingungsausdrücke finden Sie auf [Seite 153](#). Auswertungsbeispiele in Zusammenhang mit Preselection und Postselection finden Sie auf [Seite 36](#).

Der SAT-Datei-Verwalter möchte in diesem Beispiel

1. potenzielle Eindringversuche während der vorhergehenden Sitzung erkennen. Dazu selektiert er die SATLOG-Sätze abgewiesener LOGON-Versuche aus der SATLOG-Datei.
2. eine analysis-file erzeugen, die alle Ereignisse enthält, die Datei-Objekte betreffen. Diese soll zu einem späteren Zeitpunkt dezentral analysiert werden.

### Voraussetzungen

- Für alle schaltbaren Benutzerkennungen, also alle, außer denen mit dem Privileg SECURITY-ADMINISTRATION oder SAT-FILE-MANAGEMENT, wurde das Audit-Attribut auf OFF gesetzt:

```
/modify-sat-preselection user-auditing=*all-switchable(audit-switch=*off)
```

- Das Audit-Attribut aller Ereignisse, für die es verändert werden darf, wurde in der Preselection auf OFF gesetzt (siehe „[Minimierung der Anzahl protokollierter Ereignisse](#)“ auf [Seite 29](#)). Ausnahme: Das Ereignis „Userid prüfen“ (UCK) mit Ergebnis „FAILURE“ war zur Protokollierung ausgewählt:

```
/modify-sat-preselection event-auditing= -
/                                uck(audit-switch=*on(result=*failure))
```

- Die auszuwertende Sitzung hatte die Session-Nummer 137, ihr Beginn war am 1.3.2018.

Der SAT-Datei-Verwalter beginnt die Auswertung mit dem Start von SATUT:

```
/start-satut
```

```
% SAELOAD Program 'SATUT', Version '055' of '2018-03-01' loaded from file
':4V08:$SYSAUDIT.SYSLNK.SATUT.055'
% SAECOPY Copyright (C) 'Fujitsu Technology Solutions' '2018' All Rights Reserved
```

Als Eingabe-Dateien werden die SATLOG-Dateien aus der Session 137 ausgewählt:

```
//select-input-files input-files=*std(session-number=137)
```

Um sich einen Überblick über die Aktivitäten in der ausgewählten Sitzung zu verschaffen, lässt sich der SAT-Datei-Verwalter eine Statistik auf SYSOUT ausgeben:

```
//show-statistics output=*sysout
```

Er erhält folgende Ausgabe (die genaue Bedeutung der einzelnen Ausgabefelder ist bei der Anweisung //SHOW-STATISTICS auf [Seite 174](#) erklärt):

```
Input-files of statement = :PC04:$SYSAUDIT.SYS.SATLOG.2018-03-01.137.01
                        :PC04:$SYSAUDIT.SYS.SATLOG.2018-03-01.137.02
                        :PC04:$SYSAUDIT.SYS.SATLOG.2018-03-02.137.03
Begin of analyzed period : 2018/03/01 10:19:21.24
End   of analyzed period : 2018/03/02 17:44:34.23
Elapsed time              =      113113 s      =      1 d  26713 s
Records/hour              =          53.56
# of records              =          1683
Mean length               =         102.00
Mean kbytes/hour         =           5.54
```

## SUMMARY OF EVENTS

| Event-class                           | # events | # events/h |
|---------------------------------------|----------|------------|
| 1 : DMS                               |          |            |
| Files                                 | 711      | 22.63      |
| Security                              | 733      | 23.33      |
| Rename Files                          | 5        | 0.16       |
| 2 : Catalog Management                | 0        | 0.00       |
| 3 : Job Enable (Dialog & Batch)       |          |            |
| Success                               | 33       | 1.05       |
| Failure                               | 6        | 0.19       |
| 4 : Job (Rest)                        | 33       | 1.05       |
| 5 : Job Variables                     | 0        | 0.00       |
| 6 : BLS                               | 15       | 0.48       |
| 7 : Spool                             |          |            |
| Jobs                                  | 0        | 0.00       |
| Devices                               | 0        | 0.00       |
| 8 : PLAM/ILAM                         | 20       | 0.64       |
| 9 : DSSM                              |          |            |
| Connection/Disconnection              | 2        | 0.06       |
| Catalog Management                    | 17       | 0.54       |
| 10 : Syntax Files                     | 0        | 0.00       |
| 11 : Users/Groups/Privileges          |          |            |
| Users                                 | 87       | 2.77       |
| Privileges                            | 0        | 0.00       |
| Groups                                | 0        | 0.00       |
| 12 : Object Protection                |          |            |
| GUARDS                                | 0        | 0.00       |
| Coowner Protection                    | 0        | 0.00       |
| Default Protection                    | 0        | 0.00       |
| Access Control List                   | 0        | 0.00       |
| 13 : System Access Control Management |          |            |
| Terminal Sets                         | 0        | 0.00       |
| Operator Roles                        | 0        | 0.00       |
| Keys                                  | 13       | 0.41       |
| 14 : SAT                              | 2        | 0.06       |
| 15 : UTM                              | 0        | 0.00       |
| 16 : SESAM                            | 0        | 0.00       |
| 17 : POSIX                            |          |            |
| Files and Directories                 | 0        | 0.00       |
| Child Processes                       | 0        | 0.00       |
| Processes                             | 0        | 0.00       |
| System Resources                      | 0        | 0.00       |
| 18 : Communication Methods            |          |            |
| DCAM                                  | 0        | 0.00       |
| BCAM                                  | 0        | 0.00       |
| IP Security                           | 0        | 0.00       |
| 19 : Memory Pools                     | 0        | 0.00       |
| 20 : Events                           |          |            |
| Serialization                         | 0        | 0.00       |
| Eventing                              | 0        | 0.00       |
| 21 : Fast Intertask Communication     | 0        | 0.00       |
| 22 : Storage Class Events             | 0        | 0.00       |
| 23 : Data Spaces                      | 0        | 0.00       |
| 24 : Volume                           | 0        | 0.00       |
| 25 : ADAM device management           | 0        | 0.00       |
| 26 : ANY event (system exit)          | 0        | 0.00       |

| #      | EVENT | # SUCC | # FAIL | # NONE | LEN SUCC | LEN FAIL | LEN NONE | % EVENTS | % FAIL(EVENT) | RECORDS/HOUR |
|--------|-------|--------|--------|--------|----------|----------|----------|----------|---------------|--------------|
| 1      | FCD   | 59     | 0      | 0      | 108.61   | 0.00     | 0.00     | 3.51     | 0.00          | 1.88         |
| 2      | FCL   | 298    | 0      | 0      | 97.52    | 0.00     | 0.00     | 17.71    | 0.00          | 9.48         |
| 3      | FCS   | 58     | 0      | 0      | 106.02   | 0.00     | 0.00     | 3.45     | 0.00          | 1.85         |
| 4      | FDD   | 64     | 2      | 0      | 100.62   | 99.00    | 0.00     | 3.92     | 3.03          | 2.10         |
| 5      | FDS   | 64     | 20     | 0      | 103.94   | 100.50   | 0.00     | 4.99     | 23.81         | 2.67         |
| 6      | FED   | 33     | 0      | 0      | 101.09   | 0.00     | 0.00     | 1.96     | 0.00          | 1.05         |
| 7      | FMD   | 92     | 0      | 0      | 95.16    | 0.00     | 0.00     | 5.47     | 0.00          | 2.93         |
| 8      | FMS   | 11     | 0      | 0      | 121.91   | 0.00     | 0.00     | 0.65     | 0.00          | 0.35         |
| 9      | FRD   | 162    | 1      | 0      | 100.68   | 97.00    | 0.00     | 9.69     | 0.61          | 5.19         |
| 10     | FRN   | 5      | 0      | 0      | 148.60   | 0.00     | 0.00     | 0.30     | 0.00          | 0.16         |
| 11     | FRS   | 391    | 189    | 0      | 106.45   | 110.13   | 0.00     | 34.46    | 32.59         | 18.46        |
| 12     | JBE   | 16     | 2      | 0      | 81.06    | 71.50    | 0.00     | 1.07     | 11.11         | 0.57         |
| 13     | JDE   | 17     | 4      | 0      | 79.29    | 83.75    | 0.00     | 1.25     | 19.05         | 0.67         |
| 14     | JED   | 16     | 0      | 0      | 58.94    | 0.00     | 0.00     | 0.95     | 0.00          | 0.51         |
| 15     | JIN   | 17     | 0      | 0      | 69.00    | 0.00     | 0.00     | 1.01     | 0.00          | 0.54         |
| 16     | KTC   | 13     | 0      | 0      | 125.00   | 0.00     | 0.00     | 0.77     | 0.00          | 0.41         |
| 17     | LCL   | 10     | 0      | 0      | 128.50   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 18     | LEE   | 10     | 0      | 0      | 124.50   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 19     | SCR   | 14     | 3      | 0      | 79.71    | 78.33    | 0.00     | 1.01     | 17.65         | 0.54         |
| 20     | SDS   | 2      | 0      | 0      | 85.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 21     | UAD   | 2      | 0      | 0      | 81.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 22     | UCK   | 71     | 10     | 0      | 82.70    | 82.90    | 0.00     | 4.81     | 12.35         | 2.58         |
| 23     | UML   | 2      | 0      | 0      | 81.00    | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 24     | URM   | 1      | 1      | 0      | 81.00    | 81.00    | 0.00     | 0.12     | 50.00         | 0.06         |
| 25     | XLD   | 10     | 0      | 0      | 199.00   | 0.00     | 0.00     | 0.59     | 0.00          | 0.32         |
| 26     | XUL   | 5      | 0      | 0      | 80.00    | 0.00     | 0.00     | 0.30     | 0.00          | 0.16         |
| 27     | ZBG   | 3      | 0      | 0      | 245.33   | 0.00     | 0.00     | 0.18     | 0.00          | 0.10         |
| 28     | ZCH   | 2      | 0      | 0      | 130.00   | 0.00     | 0.00     | 0.12     | 0.00          | 0.06         |
| 29     | ZND   | 3      | 0      | 0      | 83.33    | 0.00     | 0.00     | 0.18     | 0.00          | 0.10         |
| TOTAL: |       | 1451   | 232    | 0      | 101.26   | 106.65   | 0.00     | 100.00   | 13.78         | 53.6         |

Der SAT-Datei-Verwalter legt die erste Auswahlbedingung mit dem Namen „badlog“ fest. Sie bezieht sich auf alle Datensätze, die das Ereignis „Userid prüfen“ mit dem Ergebnis „FAILURE“ betreffen.

```
//add-selection-conditions name=badlog, -
//                               condition=evt equal 'uck' and res equal f
```

Die zweite Auswahlbedingung namens „file“ bezieht sich auf Datensätze, in denen Ereignisse protokolliert sind, deren Kurzname mit dem Buchstaben „F“ beginnt. Das sind alle Ereignisse, die Datei-Objekte betreffen.

```
//add-selection-conditions name=file,condition=evt match 'f*'
```

Mit dem folgenden Kommando wird die Aufbereitung für beide Bedingungen in einem Schritt durchgeführt. Alle Datensätze, die der Auswahlbedingung „badlog“ genügen, werden in die Arbeitsdatei 0 geschrieben, alle Sätze, die die Bedingung „file“ erfüllen, in die Arbeitsdatei 5.

```
//start-selection from=file=*input-files, -
//                               to-file=(*parameters(condition-name=badlog), -
//                               *parameters(file=5,condition-name=file))

% SAE7001 'START-SELECTION' STATEMENT TERMINATED. '10' RECORDS SELECTED IN WORK FILE
' 0'
% SAE7001 'START-SELECTION' STATEMENT TERMINATED. '1449' RECORDS SELECTED IN WORK
FILE ' 5'
```

Es gab also 10 misslungene LOGON-Versuche und 1449 Ereignisse, die Datei-Objekte betrafen.

Die Datensätze mit den Ereignissen, die Datei-Objekte betrafen, werden zum Zweck der dezentralen Analyse in die Datei ANALYZE.FILE-EVENTS geschrieben.

```
//save-selected-records to-reduction-name=analyze.file-events,from-file=5
```

Da dem SAT-Datei-Verwalter die Anzahl der misslungenen LOGON-Versuche für eine sofortige Auswertung zu hoch erscheint, möchte er die Auswahl noch weiter einschränken. Zunächst informiert er sich über die bereits bestehenden Auswahlbedingungen.

```
//show-selection-conditions
```

```
SELECTION CONDITION NAME : BADLOG
SELECTION CONDITION      :
                          :   EVT EQUAL 'UCK'
                          :   AND RES EQUAL F
```

```
=====
SELECTION CONDITION NAME : FILE
SELECTION CONDITION      :
                          :   EVT MATCH 'F*'
=====
```

Er möchte nur die fehlerhaften LOGON-Versuche auswerten, die auf die Benutzerkennung „TSOS“ erfolgten. Dazu legt er eine weitere Auswahlbedingung fest, mit der Datensätze ausgewählt werden, die im protokollierten Datenfeld OBJ-UID den Wert TSOS enthalten (siehe „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213).

```
//add-selection-conditions name=uidtsos,condition=obj-uid equal 'tsos'
```

Dann leitet der SAT-Datei-Verwalter eine zweite Aufbereitung ein. Alle Datensätze aus der Arbeitsdatei 0, die der Bedingung „uidtsos“ genügen, sollen in die Arbeitsdatei 1 geschrieben werden. Da die Sätze in der Arbeitsdatei 0 bereits die Bedingung „badlog“ erfüllen, ist das Ergebnis dieser Aufbereitung die Menge aller Datensätze, für die beide Bedingungen („badlog“ und „uidtsos“) wahr sind.

```
//start-selection from-file=0, -
//                to-file=*parameters(file=1,condition-name=uidtsos)
```

```
% SAE7001 'START-SELECTION' STATEMENT TERMINATED. '3' RECORDS SELECTED IN WORK FILE
' 1'
```

Nur noch drei Datensätze sind das Ergebnis dieser Auswahl. Sie sollen zur Detailauswertung nach SYSLST ausgegeben werden.

```
//show-selected-records from-file=1
```

Schließlich gibt der SAT-Datei-Verwalter noch eine Statistik der Session mit Histogramm auf SYSLST aus. Dann beendet er den Auswertungslauf.

```
//show-statistics from-file=*input-files,histogram=*yes
//end
```

```
% SAE5004 SAT FILE EVALUATOR TERMINATED NORMALLY
```

## SYSLST zeigt auf den Seiten 1 und 2 das Ergebnis von //SHOW-SELECTED-RECORDS.

```

SATUT                V05.5A                2018-03-06 15:44:22                PAGE      1
PROCESSED STATEMENT : SHOW-SELECTED-RECORDS
*****
INPUT-FILES OF STATEMENT :

```

```

                :PC04:$SYSAUDIT.#SATUT.WORK-01.06.154351
SATUT                V05.5A                2018-03-06 15:44:22                PAGE      2
PROCESSED STATEMENT : SHOW-SELECTED-RECORDS
*****
EVT RES DATE      TIME   TSN  USER-ID

```

```

UCK  F  20180301 163627 0DHC TSOS  OBJ-UID= TSOS          STATION= $$$06015      PROCNAM= XYZ0231X
      F  20180302 141855 0DHG TSOS  CHKMODE= DIALOG       REJR   = 03400001
      F  20180302 141855 0DHG TSOS  AUDITID= D4C3C8C88995A97CC6E2C34BD5C5E3  OBJ-UID= TSOS
      F  20180302 144612 0DHI TSOS  STATION= $$$06007      PROCNAM= XYZ4711X      CHKMODE= NET-DIALOG-ACCESS
      F  20180302 144612 0DHI TSOS  REJR   = 02400001      PRINCCL= MCHHinz@FTS.NET
      F  20180302 144612 0DHI TSOS  AUDITID= D4C3C8D2A495A97CC6E2C34BD5C5E3  OBJ-UID= TSOS
      F  20180302 144612 0DHI TSOS  STATION= $$$06009      PROCNAM= XYZ0815X      CHKMODE= NET-DIALOG-ACCESS
      F  20180302 144612 0DHI TSOS  REJR   = 1E400001      PRINCCL= MCHKunz@FTS.NET

```

Der folgende Teil der Liste zeigt das Ergebnis von //SHOW-STATISTICS und ist weitgehend identisch mit der Statistikausgabe auf SYSOUT zu Beginn dieser Sitzung. Zusätzlich enthält er das Histogramm der Ereignisse.

SATUT V05.5A 2018-03-06 16:17:07 PAGE 1

PROCESSED STATEMENT : SHOW-STATISTICS

\*\*\*\*\*

Input-files of statement = :PC04:\$SYSAUDIT.SYS.SATLOG.2018-03-01.137.01
:PC04:\$SYSAUDIT.SYS.SATLOG.2018-03-01.137.02
:PC04:\$SYSAUDIT.SYS.SATLOG.2018-03-02.137.03
Begin of analyzed period : 2018/03/01 10:19:21.24
End of analyzed period : 2018/03/02 17:44:34.23

...

SATUT V05.5A 2018-03-06 16:17:07 PAGE 4

PROCESSED STATEMENT : SHOW-STATISTICS

\*\*\*\*\*

Table with columns for date/time and event counts. Includes a header line with a dashed line and a '#' symbol. Data rows show counts for various events like ZZ, JJJJKKSS, SSSSSSSS, SUUU, JJKUUU, UU, JJKUUU, JJUU, JJUUU, JJUU, J, J, JJJUU, FFFUU, UU.

...

Table with columns for date/time and event counts. Data rows show counts for events like FFFX, FFF, LLLLXX, FFFJJ, FFFJJJ, SSXX, FFFZ.

SATUT V05.5A 2018-03-06 16:17:07 PAGE 9

PROCESSED STATEMENT : SHOW-STATISTICS

\*\*\*\*\*

## EXPLANATION ON USED LETTERS:

-----  
 F : FCD, FCL, FCS, FDD, FDS, FED, FMD, FMS, FRD, FRN, FRS  
 J : JBE, JDE, JED, JIN  
 K : KTC  
 L : LCL, LEE  
 S : SCR, SDS  
 U : UAD, UCK, UML, URM  
 X : XLD, XUL  
 Z : ZBG, ZCH, ZND

In einer letzten, nur zum Teil mit SAT oder programmtechnisch automatisierbaren Auswertung müssen die ausgewählten Datensätze beurteilt werden, um daraus ggf. weitere Aktionen abzuleiten.

Im Beispielfall werden die ausgewählten Datensätze auf SYSLST anhand der „[Tabellen der protokollierbaren Information je Objekteignis](#)“ auf Seite 213 manuell bewertet.

| EVT | RES | DATE     | TIME   | TSN  | USER-ID |                                         |                          |                            |
|-----|-----|----------|--------|------|---------|-----------------------------------------|--------------------------|----------------------------|
| UCK | F   | 20180301 | 163627 | ODHC | TSOS    | OBJ-UID= TSOS                           | STATION= \$\$\$06015     | PROCNAM= XYZ0231X          |
|     |     |          |        |      |         | CHKMODE= DIALOG                         | REJR = 03400001          |                            |
| UCK | F   | 20180302 | 141855 | ODHG | TSOS    | AUDITID= D4C3C8C88995A97CC6E2C34BD5C5E3 |                          | OBJ-UID= TSOS              |
|     |     |          |        |      |         | STATION= \$\$\$06007                    | PROCNAM= XYZ4711X        | CHKMODE= NET-DIALOG-ACCESS |
|     |     |          |        |      |         | REJR = 02400001                         | PRINCCL= MCHHinz@FTS.NET |                            |
| UCK | F   | 20180302 | 144612 | ODHI | TSOS    | AUDITID= D4C3C8D2A495A97CC6E2C34BD5C5E3 |                          | OBJ-UID= TSOS              |
|     |     |          |        |      |         | STATION= \$\$\$06009                    | PROCNAM= XYZ0815X        | CHKMODE= NET-DIALOG-ACCESS |
|     |     |          |        |      |         | REJR = 1E400001                         | PRINCCL= MCHKunz@FTS.NET |                            |

Gemäß Tabelle für das Objekt USERID auf [Seite 272](#) werden „obj-uid“ und „chkmode“ stets protokolliert, „station“, „procnam“, „rejr“ und „princcl“ können protokolliert sein.

Eine mögliche Vorgehensweise ist nun, zu untersuchen, ob an einer bestimmten Datenstation oder im Batch eine Häufung von LOGON-Versuchen aufgetreten ist, die wegen Benutzerfehlers zurückgewiesen wurden. Dies könnte darauf hindeuten, dass versucht wurde, durch Ausprobieren von Passwörtern in das System einzudringen.

Die Analyse zeigt in diesem Fall, dass innerhalb des gesamten Auswertungszeitraums von mehr als 24 Stunden nur drei LOGON-Versuche für TSOS (obj-uid) im Dialog (chkmode) wegen Benutzerfehlers (rejr) abgewiesen wurden (siehe Tabelle auf [Seite 272](#)). Diese erfolgten zudem von unterschiedlichen Datenstationen (station und procnam). Daher würde die Analyse hier insgesamt zu dem Ergebnis „unbedenklich“ führen.

## 2.7 Tabelle der Objekteignisse

Die folgende Tabelle zeigt die Objekte und ihre protokollierbaren Ereignisse, die Kurznamen der Ereignisse und Angaben zu ihren Audit-Attributen. Der Sicherheitsbeauftragte kann mit dem Kommando /MODIFY-SAT-PRESELECTION die Audit-Attribute der meisten Ereignisse verändern.

Die Spalten der Tabelle bedeuten im Einzelnen:

- Spalte **OBJEKT Ereignis**  
Angabe des Objekts und der Operationen, die zu protokollierbaren Ereignissen führen. Die Angabe „(siehe Hinweis)“ verweist auf zusätzliche Informationen für das Objekt im Anschluss an die Tabelle.
- Spalte **Kurzname für Ereignis**  
Jedes Ereignis hat einen dreistelligen Kurznamen, der bei den Kommandos /SHOW-SAT-STATUS und /MODIFY-SAT-PRESELECTION sowie bei den Anweisungen //ADD-SELECTION-CONDITIONS und //SELECT-RECORDS als Schlüsselwort angegeben werden kann.
- Spalte **Audit-Attribut Änd**  
Gibt an, ob das Audit-Attribut für das Ereignis verändert werden kann.
 

|          |                                                                                          |
|----------|------------------------------------------------------------------------------------------|
| J (JA)   | Audit-Attribut kann verändert werden                                                     |
| N (NEIN) | Audit-Attribut kann nicht verändert werden<br>(permanent sicherheitsrelevantes Ereignis) |
| -        | Eintrag nicht relevant                                                                   |
- Spalte **Audit-Attribut Std**  
Zeigt die Standardeinstellung für das Audit-Attribut (siehe [Seite 22](#)) des Ereignisses an:
 

|   |                                                                                                                                                                      |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A | Audit-Attribut ALL, d.h. das Ereignis wird stets protokolliert                                                                                                       |
| S | Audit-Attribut SUCCESS, d.h. das Ereignis wird protokolliert, wenn es erfolgreich ausgeführt worden ist<br>(Datenfeld <code>res equal S</code> im SATLOG-Satz)       |
| F | Audit-Attribut FAILURE, d.h. das Ereignis wird protokolliert, wenn es nicht erfolgreich ausgeführt worden ist<br>(Datenfeld <code>res equal F</code> im SATLOG-Satz) |
| N | Audit-Attribut NONE, d.h. das Ereignis wird nicht protokolliert                                                                                                      |
| - | Eintrag nicht relevant                                                                                                                                               |

*Hinweis*

Die in diesem Handbuch dokumentierten Ereignisse und Felder entsprechen dem Stand zum Zeitpunkt des Erscheinens des Handbuchs. Für Produkte, die Informationen an SAT zur Protokollierung übergeben und ein späteres Erscheinungsdatum haben, kann sich Art und Umfang der protokollierten Information ändern. Für diese Produkte wird die Liste der Ereignisse und Felder im jeweiligen Produkthandbuch gepflegt. Berücksichtigen Sie deshalb vorrangig die Hinweise im jeweiligen Produkthandbuch.

| OBJEKT<br>Ereignis                                                                                                                                                                                                                           | Kurzname<br>für Ereignis        | Audit-Attribut        |                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------|-----------------------|
|                                                                                                                                                                                                                                              |                                 | Änd                   | Std                   |
| <b>ADAM</b> Geräteverwaltung<br>Eröffnen einer Gerätebedienung                                                                                                                                                                               | ADO                             | J                     | N                     |
| <b>ANY</b><br>beliebiges Ereignis (System-Exit) (siehe Hinweis)                                                                                                                                                                              | ANY                             | J                     | N                     |
| <b>APPLICATION</b> (DCAM)<br>Anwendung öffnen (YOPEN)<br>Anwendung schließen (YCLOSE)<br>Verbindung aufbauen (YOPNCON)<br>Verbindung abbauen (YCLSCON)                                                                                       | DON<br>DCL<br>DCN<br>DDS        | J<br>J<br>J<br>J      | N<br>N<br>N<br>N      |
| <b>BCAM</b><br>TSAP öffnen<br>TSAP schließen<br>Verbindung öffnen<br>Verbindung beenden                                                                                                                                                      | BAO<br>BAC<br>BCN<br>BDS        | J<br>J<br>J<br>J      | N<br>N<br>N<br>N      |
| <b>CATALOG</b> (PVS)<br>Import-Pubset-Task starten<br>Export-Pubset-Task starten<br>Katalog prüfen<br>Katalog konvertieren                                                                                                                   | CIP<br>CEP<br>CKR<br>CVR        | J<br>J<br>J<br>J      | S<br>S<br>N<br>N      |
| <b>CONSLOG</b> (siehe Hinweis)<br>CONSLOG-Eintrag                                                                                                                                                                                            | CLG                             | -                     | -                     |
| <b>COOWNER PROTECTION</b><br>Regel für Miteigentümerschutz hinzufügen<br>Regel für Miteigentümerschutz ändern<br>Miteigentümberechtigungsregel anzeigen<br>Regel für Miteigentümerschutz entfernen<br>Regel für Miteigentümerschutz anzeigen | CRA<br>CRM<br>CRQ<br>CRR<br>CRS | J<br>J<br>J<br>J<br>J | N<br>N<br>N<br>N<br>N |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 1 von 11)

| OBJEKT<br>Ereignis                             | Kurzname<br>für Ereignis | Audit-Attribut |     |
|------------------------------------------------|--------------------------|----------------|-----|
|                                                |                          | Änd            | Std |
| <b>DATA SPACES</b> (siehe Hinweis)             |                          |                |     |
| DATA SPACE erzeugen                            | DSB                      | J              | N   |
| mit DATA SPACE verbinden                       | DSC                      | J              | N   |
| Verbindung mit DATA SPACE abbrechen            | DSD                      | J              | N   |
| DATA SPACE löschen                             | DSE                      | J              | N   |
| DATA SPACE ändern/ zurücksetzen                | DSM                      | J              | N   |
| <b>DEFAULT PROTECTION</b>                      |                          |                |     |
| Standardwerte für Schutzattribute festlegen    | DAA                      | J              | N   |
| Standardwerte für Schutzattribute ändern       | DAM                      | J              | N   |
| Standardwerte für Schutzattribute anzeigen     | DAS                      | J              | N   |
| Regel für Standardschutz hinzufügen            | DRA                      | J              | N   |
| Regel für Standardschutz ändern                | DRM                      | J              | N   |
| Standardschutzattribute für Objekt anzeigen    | DRQ                      | J              | N   |
| Regel für Standardschutz entfernen             | DRR                      | J              | N   |
| Regel für Standardschutz anzeigen              | DRS                      | J              | N   |
| Benutzerkennung für Objektpfad hinzufügen      | DUA                      | J              | N   |
| Benutzerkennung für Objektpfad entfernen       | DUR                      | J              | N   |
| Benutzerkennung für Objektpfad anzeigen        | DUS                      | J              | N   |
| <b>EVENTING-ITEM</b> (siehe Hinweis)           |                          |                |     |
| Ereignissteuerung einschalten                  | EEE                      | J              | N   |
| Ereignissteuerung ausschalten                  | EDE                      | J              | N   |
| Serialisierung einschalten                     | EES                      | J              | N   |
| Serialisierung ausschalten                     | EDS                      | J              | N   |
| <b>FILE</b> (siehe Hinweis)                    |                          |                |     |
| Datei erstellen                                | FCD                      | J              | N   |
| Datei lesen                                    | FRD                      | J              | N   |
| Datei ausführen (open exec)                    | FED                      | J              | N   |
| Datei modifizieren                             | FMD                      | J              | N   |
| Datei schließen                                | FCL                      | J              | N   |
| Datei löschen                                  | FDD                      | J              | N   |
| Datei mit ARCHIVE umbenennen                   | FAR                      | J              | N   |
| Datei umbenennen                               | FRN                      | J              | N   |
| Schutzattribute erstellen                      | FCS                      | J              | N   |
| Schutzattribute modifizieren                   | FMS                      | J              | N   |
| Schutzattribute löschen                        | FDS                      | J              | N   |
| Schutzattribute lesen                          | FRS                      | J              | N   |
| Schutzattribute importieren                    | FIS                      | J              | N   |
| Schutzattribute exportieren                    | FES                      | J              | N   |
| Datei in entschlüsselte Datei umwandeln        | FDC                      | J              | N   |
| Datei in verschlüsselte Datei umwandeln        | FEC                      | J              | N   |
| File extents verschieben (SPACEOPT)            | FME                      | J              | N   |
| Objekt für Reorganisation auswählen (SPACEOPT) | FSO                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 2 von 11)

| OBJEKT<br>Ereignis                                   | Kurzname<br>für Ereignis | Audit-Attribut |     |
|------------------------------------------------------|--------------------------|----------------|-----|
|                                                      |                          | Änd            | Std |
| <b>FITC (Fast Intertask Comm.)</b> (siehe Hinweis)   |                          |                |     |
| Port Access definieren                               | POA                      | J              | N   |
| Port definieren                                      | POB                      | J              | N   |
| an Port anschließen                                  | POC                      | J              | N   |
| von Port trennen                                     | POD                      | J              | N   |
| Port freigeben                                       | POE                      | J              | N   |
| Port Access freigeben                                | POR                      | J              | N   |
| impliziter Austausch mit Port                        | POX                      | J              | N   |
| <b>GROUP</b> (user group)                            |                          |                |     |
| hinzufügen                                           | GAD                      | J              | A   |
| modifizieren                                         | GMD                      | J              | A   |
| entfernen                                            | GRM                      | J              | A   |
| anzeigen                                             | GSH                      | J              | N   |
| <b>GUARDS</b>                                        |                          |                |     |
| Guard erzeugen                                       | GUB                      | J              | N   |
| Guard kopieren                                       | GUC                      | J              | N   |
| Guard löschen                                        | GUD                      | J              | N   |
| Guardskatalog wechseln                               | GUF                      | J              | N   |
| Guardskatalog reparieren                             | GUR                      | J              | N   |
| Attribute ändern                                     | GUM                      | J              | N   |
| Attribute anzeigen                                   | GUS                      | J              | N   |
| Zugriffsbedingung definieren                         | GAA                      | J              | N   |
| Zugriffsbedingung ändern                             | GAM                      | J              | N   |
| Zugriffsbedingung löschen                            | GAR                      | J              | N   |
| Zugriffsbedingung anzeigen                           | GAS                      | J              | N   |
| Zugriffsbedingung abfragen                           | GAQ                      | J              | N   |
| <b>IPSEC</b>                                         |                          |                |     |
| IPSEC Security Datenbasis laden                      | ILD                      | J              | N   |
| Verstoß gegen die Security Policy beim Datentransfer | IPV                      | J              | N   |
| <b>JOB</b> (siehe Hinweis)                           |                          |                |     |
| Stapelauftrag oder Subtask einleiten                 | JBE                      | J              | F   |
| Auftrag abbrechen                                    | JCN                      | J              | N   |
| Dialog oder RLOGIN einleiten                         | JDE                      | J              | A   |
| Auftrag beenden                                      | JED                      | J              | N   |
| Stapelauftrag oder Subtask initiieren                | JIN                      | J              | A   |
| Stapelauftrag modifizieren                           | JMD                      | J              | N   |
| POSIX-Task erzeugen                                  | JFK                      | J              | A   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 3 von 11)

| OBJEKT<br>Ereignis                                                                                                      | Kurzname<br>für Ereignis | Audit-Attribut |     |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|-----|
|                                                                                                                         |                          | Änd            | Std |
| <b>JOB VARIABLES</b>                                                                                                    |                          |                |     |
| umbenennen mit ARCHIVE                                                                                                  | JVA                      | J              | N   |
| Schutzattribute erstellen                                                                                               | JVC                      | J              | N   |
| Schutzattribute löschen                                                                                                 | JVD                      | J              | N   |
| Schutzattribute modifizieren                                                                                            | JVM                      | J              | F   |
| Daten lesen (GETJV)                                                                                                     | JVG                      | J              | F   |
| Daten schreiben (SETJV)                                                                                                 | JVS                      | J              | F   |
| JV abfragen                                                                                                             | JVQ                      | J              | N   |
| JV umbenennen                                                                                                           | JVR                      | J              | N   |
| <b>KEY</b>                                                                                                              |                          |                |     |
| KERBEROS Encryption Type hinzufügen                                                                                     | KEA                      | J              | A   |
| KERBEROS Encryption Type löschen                                                                                        | KED                      | J              | A   |
| KERBEROS Principal hinzufügen                                                                                           | KPA                      | J              | A   |
| KERBEROS Principal löschen                                                                                              | KPD                      | J              | A   |
| KERBEROS Principal ändern                                                                                               | KPM                      | J              | A   |
| KERBEROS Ticket Check                                                                                                   | KTC                      | J              | F   |
| Fehlversuch bei der Crypto-Kennwort-Überprüfung<br>nach Überschreitung der maximal erlaubten Anzahl<br>an Fehlversuchen | KXM                      | J              | F   |
| <b>MEMORY-POOL</b> (siehe Hinweis)                                                                                      |                          |                |     |
| eröffnen (ENAMP)                                                                                                        | MEN                      | J              | N   |
| schließen (DISMP)                                                                                                       | MDS                      | J              | N   |
| freigeben (RELMP)                                                                                                       | MRL                      | J              | N   |
| lesbar machen für TU (mit (\$)CSTMP in TPR)                                                                             | MRD                      | J              | N   |
| Lesbarkeit ändern mit CSTMP in TU                                                                                       | MAC                      | J              | S   |
| <b>OPERATOR ROLE</b>                                                                                                    |                          |                |     |
| Routing Code hinzufügen                                                                                                 | ORA                      | J              | N   |
| Operator Role erzeugen                                                                                                  | ORB                      | J              | N   |
| Operator Role zuweisen                                                                                                  | ORC                      | J              | N   |
| Operator Role aus Benutzersatz entfernen                                                                                | ORD                      | J              | N   |
| Operator Role löschen                                                                                                   | ORE                      | J              | N   |
| Routing-Code entziehen                                                                                                  | ORR                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 4 von 11)

| OBJEKT<br>Ereignis                               | Kurzname<br>für Ereignis | Audit-Attribut |     |
|--------------------------------------------------|--------------------------|----------------|-----|
|                                                  |                          | Änd            | Std |
| <b>PLAM</b>                                      |                          |                |     |
| Bibliothekselement erstellen                     | LCE                      | J              | N   |
| Bibliothekselement modifizieren                  | LME                      | J              | N   |
| Bibliothekselement lesen                         | LRE                      | J              | N   |
| Bibliothekselement ausführen                     | LEE                      | J              | N   |
| Bibliothekselement schließen                     | LCL                      | J              | N   |
| Bibliothekselement löschen                       | LDE                      | J              | N   |
| Bibliothekselement umbenennen                    | LRN                      | J              | N   |
| Sicherheitsattribut erzeugen                     | LCS                      | J              | N   |
| Sicherheitsattribut löschen                      | LDS                      | J              | N   |
| Sicherheitsattribut verändern                    | LMS                      | J              | N   |
| <b>POSIX-CHILD-Process</b> (siehe Hinweis)       |                          |                |     |
| Neuen Prozess erzeugen (fork)                    | XFK                      | J              | N   |
| Neuen Prozess bei rlogin-Zugang erzeugen (rfork) | XRF                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 5 von 11)

| OBJEKT<br>Ereignis                                                           | Kurzname<br>für Ereignis | Audit-Attribut |     |
|------------------------------------------------------------------------------|--------------------------|----------------|-----|
|                                                                              |                          | Änd            | Std |
| <b>POSIX-FILE-and-Directory</b> (siehe Hinweis)                              |                          |                |     |
| Aktuelles Dateiverzeichnis wechseln (chdir)                                  | XCD                      | J              | N   |
| Datei schließen (close)                                                      | XCL                      | J              | N   |
| Dateizugriffsrechte ändern (chmod)                                           | XCM                      | J              | N   |
| Eigentümer oder Gruppe einer Datei ändern (chown)                            | XCO                      | J              | N   |
| Neue Datei erzeugen (creat)                                                  | XCR                      | J              | N   |
| Verzeichnis via Deskriptor erzeugen (mkdirat)                                | XDA                      | J              | N   |
| Dateideskriptor duplizieren (dup)                                            | XDP                      | J              | N   |
| Kontrolloperation auf Dateien (fcntl)                                        | XFC                      | J              | N   |
| Aktuelles Dateiverzeichnis wechseln via Deskriptor (fchdir)                  | XFD                      | J              | N   |
| Dateizugriffsrechte ändern via Deskriptor (fchmod)                           | XFM                      | J              | N   |
| Eigentümer oder Gruppe einer Datei ändern via Deskriptor (fchown)            | XFO                      | J              | N   |
| Link zu einer Datei via Deskriptor erzeugen (linkat)                         | XLA                      | J              | N   |
| Verweis auf eine Datei erzeugen (link)                                       | XLN                      | J              | N   |
| Eigentümer oder Gruppe einer Datei oder eines Verweises ändern (lchown)      | XLO                      | J              | N   |
| Dateizugriffsrechte via Deskriptor ändern (fchmodat)                         | XMA                      | J              | N   |
| Dateiverzeichnis erzeugen (mkdir)                                            | XMD                      | J              | N   |
| Abbildung Datei in virtuellen Speicher (mmap)                                | XMM                      | J              | N   |
| Schutzattribute für Abbildung Datei in virtuellen Speicher setzen (mprotect) | XMP                      | J              | N   |
| Dateisystem einhängen (mount)                                                | XMT                      | J              | N   |
| Abbildung Datei in virtuellen Speicher aufheben (munmap)                     | XMU                      | J              | N   |
| Datei via Deskriptor öffnen (openat)                                         | XOA                      | J              | N   |
| Datei öffnen (open)                                                          | XOP                      | J              | N   |
| Dateiname via Deskriptor ändern (renameat)                                   | XRA                      | J              | N   |
| Dateiverzeichnis löschen (rmdir)                                             | XRD                      | J              | N   |
| Dateiname ändern (rename)                                                    | XRN                      | J              | N   |
| Symbolischen Verweis auf eine Datei via Deskriptor erzeugen (symlinkat)      | XSA                      | J              | N   |
| Symbolischen Verweis auf eine Datei erzeugen (symlink)                       | XSL                      | J              | N   |
| Datei oder Verzeichnis via Deskriptor löschen (unlinkat)                     | XUA                      | J              | N   |
| Dateibitmaske für einen Prozess setzen (umask)                               | XUM                      |                | N   |
| Datei löschen (remove/unlink)                                                | XUN                      | J              | N   |
| Dateisystem aushängen (umount)                                               | XUT                      | J              | N   |
| Gruppe oder Besitzer einer Datei via Deskriptor ändern (fchownat)            | XWA                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 6 von 11)

| OBJEKT<br>Ereignis                                                               | Kurzname<br>für Ereignis | Audit-Attribut |     |
|----------------------------------------------------------------------------------|--------------------------|----------------|-----|
|                                                                                  |                          | Änd            | Std |
| <b>POSIX-PROCESS</b> (siehe Hinweis)                                             |                          |                |     |
| Effektive Gruppennummer eines Prozesses setzen (setegid)                         | XEG                      | J              | N   |
| Effektive Benutzernummer eines Prozesses setzen (seteuid)                        | XEU                      | J              | N   |
| Datei ausführen (exec)                                                           | XEX                      | J              | N   |
| Maximalmenge von Gruppenmitgliedschaften für einen Prozess festlegen (setgroups) | XGR                      | J              | N   |
| Signal an Prozess oder Prozessgruppe senden (kill)                               | XKL                      | J              | N   |
| Prozessgrenzen setzen (ulimit)                                                   | XLM                      | J              | N   |
| Reale und effektive Gruppennummer eines Prozesses setzen (setregid)              | XRG                      | J              | N   |
| Reale und effektive Benutzernummer eines Prozesses setzen (setreuid)             | XRU                      | J              | N   |
| Gruppennummer eines Prozesses setzen (setgid)                                    | XSG                      | J              | N   |
| Prozessgruppennummer einstellen (setpgpr)                                        | XSP                      | J              | N   |
| Grenzwert für ein Betriebsmittel einstellen (setrlimit)                          | XSR                      | J              | N   |
| Benutzernummer eines Prozesses setzen (setuid)                                   | XSU                      | J              | N   |
| <b>POSIX-SYSTEM-Resources</b> (siehe Hinweis)                                    |                          |                |     |
| Systemzeit modifizieren (adjtime)                                                | XAJ                      | J              | N   |
| Benutzerattribute setzen (pwent)                                                 | XPW                      | J              | N   |
| Semaphor-Steueroperationen (semsys)                                              | XSE                      | J              | N   |
| Shared-Memory-Steueroperationen (shmsys)                                         | XSH                      | J              | N   |
| <b>PRIVILEGE</b>                                                                 |                          |                |     |
| vergeben                                                                         | PST                      | N              | A   |
| entziehen                                                                        | PRT                      | N              | A   |
| Sammelprivileg erzeugen                                                          | PSC                      | J              | S   |
| Sammelprivileg löschen                                                           | PSD                      | J              | S   |
| Privileg zu Sammelprivileg hinzufügen                                            | PSA                      | N              | A   |
| Privileg aus Sammelprivileg entfernen                                            | PSR                      | N              | A   |
| <b>PROGRAM</b> (siehe Hinweis)                                                   |                          |                |     |
| laden/ausführen                                                                  | XLD                      | J              | N   |
| entladen                                                                         | XUL                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 7 von 11)

| OBJEKT<br>Ereignis                                  | Kurzname<br>für Ereignis | Audit-Attribut |     |
|-----------------------------------------------------|--------------------------|----------------|-----|
|                                                     |                          | Änd            | Std |
| <b>SAT</b> (siehe Hinweis)                          |                          |                |     |
| Kommando HOLD-SAT-LOGGING                           | ZHO                      | N              | A   |
| Kommando RESUME-SAT-LOGGING                         | ZRE                      | N              | A   |
| Kommando MODIFY-SAT-PRESELECTION                    | ZPS                      | N              | A   |
| Kommando MODIFY-SAT-SUPPORT-<br>PARAMETERS          | ZMS                      | N              | A   |
| Kommando CHANGE-SAT-FILE                            | ZCH                      | N              | A   |
| Kommando SAVE-SAT-PARAMETERS                        | ZSP                      | N              | A   |
| SATLOG-Datei öffnen (HEADER-Satz)                   | ZBG                      | N              | A   |
| SATLOG-Datei schließen (TRAILER-Satz)               | ZND                      | N              | A   |
| SAT Event Preselection                              | ZEP                      | N              | A   |
| <b>SAT-ALARM</b>                                    |                          |                |     |
| Kommando ADD-SAT-ALARM-CONDITIONS                   | ZCA                      | N              | A   |
| Kommando REMOVE-SAT-ALARM-CONDITIONS                | ZDA                      | N              | A   |
| Kommando MODIFY-SAT-ALARM-CONDITIONS                | ZMA                      | N              | A   |
| SAT Alarm auslösen                                  | ZAL                      | N              | A   |
| <b>SAT-FILTER</b>                                   |                          |                |     |
| Kommando ADD-SAT-FILTER-CONDITIONS                  | ZCF                      | N              | A   |
| Kommando REMOVE-SAT-FILTER-CONDITIONS               | ZDF                      | N              | A   |
| Kommando MODIFY-SAT-FILTER-CONDITIONS               | ZMF                      | N              | A   |
| <b>SESAM</b> (siehe Hinweis)                        |                          |                |     |
| DBH-Session administrieren                          | SEA                      | J              | N   |
| Zugriffsrechte und Benutzerzugänge ändern           | SEP                      | J              | N   |
| DDL-, SSL-, Utility-Anweisung                       | SES                      | J              | N   |
| SESAM-Task (DBH- oder Service-Task) starten/beenden | SET                      | J              | N   |
| Vorgang beenden                                     | SEU                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 8 von 11)

| OBJEKT<br>Ereignis                                  | Kurzname<br>für Ereignis | Audit-Attribut |     |
|-----------------------------------------------------|--------------------------|----------------|-----|
|                                                     |                          | Änd            | Std |
| <b>SMS (System Managed Storage)</b>                 |                          |                |     |
| Speicherklasse einrichten                           | SCC                      | J              | N   |
| Eigenschaften der Speicherklasse ändern             | SCM                      | J              | N   |
| Speicherklasse löschen                              | SCD                      | J              | N   |
| Speicherklasse an volume-set-list koppeln           | SCB                      | J              | N   |
| PVSREN: alle Speicherklassen löschen                | SCP                      | J              | N   |
| Speicherklasse von volume-set-list entkoppeln       | SCU                      | J              | N   |
| Kommando CHANGE-STORAGE-CLASS-CATALOG               | SCX                      | J              | N   |
| volume-set-list einrichten                          | VLC                      | J              | N   |
| volume-set-list ändern                              | VLM                      | J              | N   |
| volume-set-list löschen                             | VLD                      | J              | N   |
| Datenträger in volume-set-list eintragen            | VLA                      | J              | N   |
| Datenträger aus volume-set-list entfernen           | VLR                      | J              | N   |
| Kommando<br>CHANGE-VOLUME-SET-LIST-CATALOG          | VLX                      | J              | N   |
| PVSREN: volume-set umbenennen                       | VP1                      | J              | N   |
| PVSREN: alle volume-sets umbenennen                 | VP2                      | J              | N   |
| PVSREN: alle volume-set-lists löschen               | VP3                      | J              | N   |
| <b>SPOOL DEVICE</b>                                 |                          |                |     |
| RSO-Gerät definieren                                | SDA                      | J              | N   |
| Eigenschaften ändern                                | SDM                      | J              | N   |
| Eintrag löschen                                     | SDR                      | J              | N   |
| <b>SPOOL JOBS</b> (siehe Hinweis)                   |                          |                |     |
| Druck anfordern                                     | JPR                      | J              | N   |
| Job löschen                                         |                          | J              | N   |
| Druck beendet                                       | JPC                      | J              | N   |
| Job unterbrechen                                    | JPE<br>JPI               | J              | N   |
| <b>SUBSYSTEM</b> (siehe Hinweis)                    |                          |                |     |
| aktivieren                                          | SCR                      | J              | A   |
| deaktivieren                                        | SDL                      | J              | A   |
| anhalten                                            | SHD                      | J              | A   |
| Subsystem entfernen                                 | SRM                      | J              | A   |
| fortsetzen                                          | SRS                      | J              | A   |
| Konnektierung mit nicht privilegiertem Subsystem    | SCN                      | J              | N   |
| Diskonnektierung von nicht privilegiertem Subsystem | SDS                      | J              | N   |
| Katalogverwaltung                                   | SCT                      | J              | A   |
| Subsystem-Teil laden                                | SLP                      | J              | N   |
| Subsystem-Datei wechseln                            | SFC                      | J              | N   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 9 von 11)

| OBJEKT<br>Ereignis                      | Kurzname<br>für Ereignis | Audit-Attribut |     |
|-----------------------------------------|--------------------------|----------------|-----|
|                                         |                          | Änd            | Std |
| <b>SYNTAX FILE</b>                      |                          |                |     |
| aktivieren                              | YAC                      | J              | N   |
| modifizieren                            | YMD                      | J              | N   |
| Hierarchie eröffnen (Makro OPNCALL)     | YON                      | J              | N   |
| für Subsystem aktivieren                | YAD                      | J              | N   |
| überprüfen                              | YCK                      | J              | N   |
| <b>TAPE encryption</b>                  |                          |                |     |
| Anweisung CREATE-ENCRYPTION-KEY         | TKC                      | J              | A   |
| Anweisung ADD-ENCRYPTION-KEY            | TKA                      | J              | A   |
| Anweisung COPY-ENCRYPTION-KEYS          | TKP                      | J              | A   |
| Anweisung REMOVE-ENCRYPTION-KEYS        | TKR                      | J              | A   |
| Anweisung SHOW-ENCRYPTION-KEYS          | TKS                      | J              | N   |
| Anweisung SET-WRITE-ENCRYPTION-KEY      | TWK                      | J              | A   |
| Anweisung DELETE-KEY-BOX                | TBD                      | J              | A   |
| Anweisung EXPORT-KEY-BOX                | TBE                      | J              | A   |
| Anweisung IMPORT-KEY-BOX                | TBI                      | J              | A   |
| Anweisung REPAIR-KEY-BOX                | TBR                      | J              | N   |
| Anweisung MODIFY-VOLUME-ENCRYPTION-ATTR | TVM                      | J              | A   |
| Anweisung SHOW-VOLUME-ENCRYPTION-ATTR   | TVS                      | J              | N   |
| Zugriff auf key box                     | TBA                      | J              | A   |
| <b>TERMINAL SET</b>                     |                          |                |     |
| erzeugen                                | TSB                      | J              | N   |
| kopieren                                | TSC                      | J              | N   |
| löschen                                 | TSD                      | J              | N   |
| ändern                                  | TSM                      | J              | N   |
| <b>USERID</b> (siehe Hinweis)           |                          |                |     |
| hinzufügen                              | UAD                      | J              | A   |
| Attribute modifizieren                  | UMD                      | J              | N   |
| entfernen                               | URM                      | J              | A   |
| sperrern                                | ULK                      | J              | N   |
| entsperren                              | UUL                      | J              | S   |
| prüfen                                  | UCK                      | J              | F   |
| Schutzattribute festlegen               | USL                      | J              | A   |
| Schutzattribute modifizieren            | UML                      | J              | A   |
| Kennwortschutz modifizieren             | UMP                      | J              | A   |
| Kommando REQUEST-OPERATOR-ROLE          | UOP                      | J              | A   |
| Kommando MODIFY-POSIX-USER-ATTRIBUTES   | UPA                      | J              | N   |
| Kommando MODIFY-POSIX-USER-DEFAULTS     | UPD                      | J              | N   |
| Kommando MODIFY-USER-PUBSET-ATTRIBUTES  | UUP                      | J              | A   |
| Kommando MODIFY-LOGON-DEFAULTS          | UDM                      | J              | A   |
| Kommando SET-LOGON-DEFAULTS             | UDS                      | J              | A   |
| Kommando UNLOCK-USER-SUSPEND            | UUS                      | J              | A   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 10 von 11)

| OBJEKT<br>Ereignis                              | Kurznamen<br>für Ereignis | Audit-Attribut |     |
|-------------------------------------------------|---------------------------|----------------|-----|
|                                                 |                           | Änd            | Std |
| <b>UTM-Ereignisse</b> (siehe Hinweis)           | TRM                       | J              | A   |
| <b>VOLUME (MAREN)</b> (siehe Hinweis)           |                           |                |     |
| Verwalter ändert Attribute                      | VMA                       | J              | N   |
| Datenträger entfernen                           | VRM                       | J              | N   |
| Datenträger hinzufügen                          | VAD                       | J              | N   |
| Benutzer ändert Attribute                       | VMU                       | J              | N   |
| Benutzer bearbeitet Datenträger                 | VVP                       | J              | N   |
| MAREN-Parameter ändern                          | VMM                       | J              | N   |
| Datenträger Attribute anzeigen                  | VSA                       | J              | N   |
| MAREN-Parameter anzeigen                        | VSP                       | J              | N   |
| <b>VOLUME (andere Produkte)</b> (siehe Hinweis) |                           |                |     |
| Datenträger öffnen                              | VON                       | J              | N   |
| Datenträger schließen                           | VCL                       | J              | N   |
| geschützten Datenträger initialisieren          | VIP                       | J              | A   |
| ungeschützten Datenträger initialisieren        | VIN                       | J              | N   |
| Platte initialisieren                           | VID                       | J              | A   |
| IOCF installieren                               | VIO                       | J              | N   |
| Datenträger anfordern (FDDRL)                   | VDA                       | J              | S   |
| Datenträger freigeben (FDDRL)                   | VDR                       | J              | N   |
| Datenträger ändern (FDDRL)                      | VDU                       | J              | S   |

Tabelle 4: Objekt-Ereignisse, Kurznamen und Audit-Attribute (Teil 11 von 11)

## Hinweise zu Objekten und ihren Ereignissen

### *Hinweis zu ANY events*

Der Sicherheitsbeauftragte und der SAT-Datei-Verwalter können über den System Exit 110 mit Hilfe des Makros \$SATANY eigene Informationen über ein Ereignis, das protokolliert wird, in die SATLOG-Datei schreiben (siehe [Abschnitt „Verfeinern der Auswahl mit System-Exit Nr.110“ auf Seite 32](#)).

### *Hinweis zu CONSLOG*

CLG sind keine protokollierbaren Ereignisse.

Für die SATUT-Auswertung können jedoch auch CONSLOG-Protokolldateien im Standardformat als Eingabedateien verwendet werden. Ihre Einträge werden zur Auswertung in CLG-Datensätze umgewandelt und können so in die Selektion einbezogen werden. Der Inhalt des Protokolldatensatzes hängt vom Typ der CONSLOG-Meldung ab (siehe [Seite 221](#)).

*Hinweis zu DATA SPACES*

Operationen im privilegierten Zustand (TPR) werden nicht protokolliert. Wenn SCOPE=LOCAL verwendet wird, wird der Mißerfolg des Kommandos protokolliert.

*Hinweis zu EVENTING-ITEM*

Bei SCOPE = LOCAL wird nicht protokolliert.

*Hinweis zu FILE und FITC*

1. Bei aktiviertem Audit-Attribut werden für eine Datei alle Zugriffe und Zugriffsversuche protokolliert, wenn der Wert des Audit-Attributs und das Ereignis-Ergebnis übereinstimmen (siehe [Abschnitt „Subjekt, Objekt und Ereignis“ auf Seite 16](#)).
2. Folgende Merkmale einer Datei sind sicherheitsrelevant: user-access, access, audit, passwords, retention period, einfache Zugriffskontrollliste. Da die Systemverwaltung unter TSOS Kennwörter im Katalogeintrag lesen kann, ist dieses Ereignis (read-password) sicherheitsrelevant.
3. Beim Löschen einer Datei können zwei Ereignisse protokolliert werden:
  - Löschen von Daten (delete data)
  - Löschen des Katalogeintrags (delete security attributes)

Das gleiche gilt für die Umbenennung einer Datei mit gleichzeitigem Ändern der Schutzmerkmale.

4. Werden in Programmen alle Dateien mit einem Befehl geschlossen, wird dieses Ereignis ('Datei schließen') für jede betroffene Datei gesondert protokolliert.
5. In Mehrrechnersystemen übernimmt der Rechner die Protokollierung, von dem aus die Datei eröffnet wurde. Im Gegensatz dazu wird die Überprüfung der Mehrbenutzbarkeit und der Zugriffsrechte auf dem Rechner durchgeführt, auf dem die Datei katalogisiert ist.
6. Da eine ARCHIVE Sub-Task das Subject Identification Interface (SID) verwendet, werden alle Datei-Ereignisse so behandelt, als gehörten sie zur Main-Task und werden protokolliert [5]. Zusätzlich gibt es ein ARCHIVE-spezifisches Ereignis, 'Datei umbenennen', das protokolliert wird.
7. Das Ereignis FSO dient zur Protokollierung der Anforderung des Benutzers, d.h. des Auftrags an SPACEOPT.

Das Ereignis FME dient zur Protokollierung des Ergebnisses der Auftragsbearbeitung.

Zu einem Satz mit dem Ereignis FSO kann es keinen, einen oder mehrere zugehörige Sätze mit dem Ereignis FME geben, je nachdem, ob und ggf. wieviele Dateien im Zuge der Auftragsbearbeitung verschoben wurden.

Umgekehrt ist einem Satz mit dem Ereignis FME immer ein Satz mit dem Ereignis FSO vorausgegangen.

*Hinweis zu JOB*

1. Wenn Aufträge, die sich noch im Wartezustand befinden, wieder gelöscht werden, werden sie nur über das Kommando CANCEL protokolliert.
2. Druck-Aufträge werden bei den entsprechenden Kommandos protokolliert (siehe SPOOL JOBS).
3. Job-Klassen sind für die SAT-Protokollierung nicht relevant.
4. In Mehrrechnersystemen werden REMOTE ENTER und REMOTE CANCEL im Zielrechner protokolliert. Im Gegensatz dazu wird ein OPEN im Ausgangs-Rechner protokolliert.
5. Das Ereignis 'Beenden von Aufträgen' (JED) wird von SAT nicht standardmäßig protokolliert, weil es bereits von CONSLOG und Accounting protokolliert wird.

*Hinweis zu MEMORY-POOL*

1. Im privilegierten Zustand (TPR) wird nur das Ereignis 'lesbar machen für TU' protokolliert.
2. Bei SCOPE = LOCAL Memory Pools werden nur die Ereignisse 'Lesbarkeit ändern' und 'lesbar machen für TU' protokolliert.

*Hinweis zu POSIX-...*

Eine Protokollierung der Ereignisse für POSIX-CHILD-Process, POSIX-FILE-and-Directo-ry, POSIX-PROCESS und POSIX-System-Resources findet nur statt, wenn der SAT-Sup-  
port für diese Ereignisse eingeschaltet wurde:

```
/MODIFY-SAT-SUPPORT-PARAMETERS POSIX-EVENTS=*ENABLED
```

*Hinweis zu PROGRAM*

Im Falle von SLICE OVERLOADING wird keine SAT-Protokollierung vorgenommen.

*Hinweis zu SAT-Ereignisse*

SAT-Ereignisse werden immer protokolliert. Ihre Protokollierung kann auch über die Auswahl nicht abgeschaltet werden. Die SATLOG-Dateien enthalten einen Header- und einen Trailer-Satz, der den besonderen Ereignissen 'Beginn der SATLOG-Datei' (ZBG) und 'Ende der SATLOG-Datei' (ZND) entspricht. ZBG- und ZND-Ereignisse werden ebenfalls immer protokolliert und können über die Auswahl nicht abgeschaltet werden.

In den von SATUT erzeugten Auswertungsdateien wird ein Header-Satz erzeugt, der dem Ereignis 'Erstellen einer Auswertungsdatei' entspricht (ZRR für replacement-files, ZRA für analysis-files).

Jedes Ereignis, welches mit der Alarm- oder Filterdefinition verbunden ist, wird ebenfalls protokolliert (ZCA, ZDA, ZMA, ZAL, ZCF, ZDF, ZMF). Die Sicherung der SAT-Parameter-Datei gehört dazu (ZSP).

*Hinweis zu SESAM*

SESAM/SQL-Server stellt dem SESAM-Verwalter Optionen zur Verfügung, mit denen er für SESAM die SAT-Protokollierung ein- und ausschalten kann. D.h. SESAM-Ereignisse können nur bei Einsatz von SESAM/SQL-Server auftreten, und auch dann nur, wenn die SAT-Protokollierung von SESAM eingeschaltet ist. In allen anderen Fällen sind die Einstellungen der SAT-Preselection hinsichtlich der SESAM- Ereignisse wirkungslos.

Um eine Protokollierung der SESAM-Ereignisse zu erreichen, müssen also sowohl die SAT-Protokollierung in SESAM als auch die SESAM-Ereignisse bei der SAT-Preselection eingeschaltet sein.

Nähere Informationen zu den SESAM-Optionen finden sich im Handbuch „SESAM/SQL-Server – Datenbankbetrieb“ [33].

*Hinweis zu SPOOL JOBS*

Es wird nur protokolliert, dass /PRINT- und /CANCEL-Kommandos verwendet wurden. Die Verarbeitung der Kommandos wird nicht protokolliert.

*Hinweis zu SUBSYSTEM*

1. Wenn vor SYSTEM READY ein Subsystem aktiviert wird, wird dieses Ereignis nicht protokolliert. Sicherheit wird jedoch durch den Zugang „Sicherer Systemstart“ siehe Handbuch „Systeminstallation“ [3] gewährleistet.
2. Wenn auf ein Subsystem zugegriffen wird, wird die Zugriffsanforderung protokolliert. Die Operationen des Subsystems werden nicht protokolliert (diese laufen unter einer anderen TSN ab).
3. Es werden nur Verbindungs- bzw. Abbrucharforderungen an nicht-privilegierte Subsysteme protokolliert; diese müssen zusätzlich erfolgreich sein.

*Hinweis zu USERID*

1. Eine Veränderung der Erlaubnis zum Aktivieren des AUDIT-Modus (Ereignis UAD oder UMD) ist aus den protokollierten Daten nicht ersichtlich.
2. Das Zurückweisen von Dialog- und Stapelaufträgen wird nur durch das Ereignis 'prüfen' der Benutzererkennung protokolliert, da dabei andere sicherheitsrelevante Ereignisse nicht auftreten.

*Hinweis zu UTM-Ereignisse*

Das Subjekt eines UTM-Ereignisses ist meistens keine BS2000-Benutzererkennung. Deshalb behandelt SAT solche Ereignisse auf andere Weise.

SAT erkennt nur ein UTM-Ereignis. Die protokollierte Information enthält einen Subcode für die einzelnen UTM-Ereignisse.

Ausführliche Informationen zur SAT-Protokollierung unter openUTM finden Sie im openUTM-Handbuch „Anwendungen generieren“ [17].

*Hinweis zu VOLUME*

1. Für Magnetbänder wird nicht protokolliert, ob der Schreibring vorhanden ist oder nicht.
2. SAT protokolliert, wenn ein Magnetband über DVS (siehe Handbuch „Einführung in das DVS“ [6]), FDDRL (siehe Handbuch „FDDRL“ [9]) oder INIT (siehe Handbuch „Dienstprogramme“ [14]) reserviert wird. Wenn ein Magnetband initialisiert wird, ist die VSN unbekannt.
3. Die Anweisung SHOW-VOLUME-ATTRIBUTES wird nur für Benutzeraufträge unter TSOS oder solche mit dem Privileg Bandverwaltung als sicherheitsrelevantes Ereignis angesehen.

MAREN-Parameter sind die mit der MAREN-Anweisung MODIFY-MAREN-PARAMETERS zu verändernden Parameter.

## 2.8 Tabellen der protokollierbaren Information je Objekt ereignis

Die folgenden Tabellen zeigen für jedes Objekt zunächst die Liste seiner Ereignisse mit den zugehörigen Informationsfeldern und der Art ihrer Ausgabe

M = Mandatory (wird ausgegeben)

O = Optional (kann erscheinen)

E = \*EXTENDED-Feld (wird nur ausgegeben, wenn mit dem Kommando /MODIFY-SAT-PRESELECTION LOGGING-QUANTITY=\*EXTENDED eingestellt wurde)

- = wird nicht ausgegeben

Die jeweils angeschlossene Tabelle zeigt, welcher Wert im jeweiligen Feld stehen kann.

Die Feldnamen, die auch über die Alarm-Funktion von SAT überwacht werden können oder für die eine Filterbedingung definiert werden kann, sind in der 2. Spalte (Al/Fil) mit einem Stern (\*) oder Pluszeichen (+) gekennzeichnet. Mit Plus (+) gekennzeichnete Felder können nur auf ihre Existenz überprüft werden (VALUE=\*ALL). Das Kennzeichen Stern (\*) bedeutet, dass auch der Inhalt des Feldes überprüft werden kann. Falls sich der Datentyp für SAT-ALARM und SAT-FILTER von dem für SATUT unterscheidet, ist der Datentyp für SAT-ALARM und SAT-FILTER in Klammern () angegeben.

Mit dem Identifikator in der 3. Spalte kann bei Verwendung der Exit-Routine Nr. 110 die SAT-Information in den protokollierten Datensätzen bearbeitet werden. Die Identifikatoren sind in sedezimaler Schreibweise angegeben.

In jedem SATLOG-Satz werden folgende Felder unabhängig vom Objekt stets versorgt:

- Benutzerkennung und TSN des Subjekts (user-id, tsn)
- Protokollierzeit (timestp)
- Kurzname für das Ereignis (evt) und Ergebnis des Ereignisses (res).  
Das Ereignis wird immer und das Ergebnis (S = Success, F = Failure) nur dann in den Tabellen dargestellt, wenn von dessen Inhalt abhängt, was im variablen Teil des SATLOG-Satzes protokolliert wird.

Abhängig von ihrer Existenz, jedoch unabhängig vom Objekt, werden folgende Felder stets versorgt:

- Das Feld auditid. Es enthält
  - die persönliche Benutzerkennung, wenn für eine Benutzerkennung der Zugang mittels persönlicher Identifizierung festgelegt ist.
 Falls es keine persönliche Benutzerkennung gibt:
  - die ersten acht Zeichen des Kerberos-Principal, wenn die Authentisierung bei \$DIALOG über Kerberos vorgenommen wurde

- Gruppenkennung (groupid)

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter  |
|----------|---------|------|----------------------------------------------------------------------------|
| auditid  | *       | 0001 | Audit subject identification<br>type: x-string 2..32                       |
| evt      |         | 00F3 | Event-type id<br>type: c-string 1..3                                       |
| groupid  | *       | 0002 | Group subject identification (user-group)<br>type: c-string 1..8           |
| res      |         | 00F5 | Event result<br>keywords: F/S                                              |
| timestp  |         | 00F1 | Time (date and time of the record creation)<br>Format: yyyy-mm-dd/hh:mm:ss |
| tsn      |         | 00F4 | TSN subject<br>type: c-string 1..4                                         |
| user-id  |         | 00F6 | user subject identification<br>type: c-string 1..8 (user-id)               |

Diese Felder werden daher in den objektspezifischen Tabellen nicht mehr erwähnt.

*Hinweise*

Bei Ereignissen des Objekts BCAM gibt es unter Umständen keine relevante Verursachertask. Die Inhalte der Datenfelder user-id und tsn sind in diesem Fall ohne Bedeutung. In das Datenfeld user-id wird dabei die Zeichenkette '(BCAM)' eingetragen.

Beim IPSEC-Ereignis „Verstoß gegen die Security Policy beim Datentransfer“ (IPV) gibt es keine relevante Verursachertask. Die Inhalte der Datenfelder user-id und tsn sind in diesem Fall ohne Bedeutung. In das Datenfeld user-id wird dabei die Zeichenkette '(IPSEC)' eingetragen.

Bei Feldern der SAT-Objekte POSIX-FILE-and-Directory, POSIX-CHILD-Process, POSIX-PROCESS und POSIX-SYSTEM-Resources kann es u.U. vorkommen, dass bei fehlerhaften Eingaben des POSIX-Anwenders Fragezeichen (d.h. '??') als Feldwert im SATLOG-Protokoll angezeigt werden.

Enthält das Datenfeld user-id die Zeichenkette '(OPR)', so ist der Verursacher des Ereignisses eine Systemtask des Operating.

Bei den Feldern `eltvers` (Version eines Bibliothekselements) und `ldvers` (Version eines geladenen Moduls) ist zu beachten, dass die größte mögliche Version nicht - wie z.B. von LMS - in das Zeichen `@` umgesetzt wird, sondern ihre interne Codierung `X'FF'` behält. Zur Abfrage in SATUT muss daher, abhängig vom eingestellten Zeichensatz, das Zeichen `ß` oder `~` verwendet werden.

## Objekt ADAM (nur bis BS2000 OSD/XC V10.0)

| Ereignis                       | evt | SAT-Information |         |
|--------------------------------|-----|-----------------|---------|
|                                |     | device          | devtype |
| Eröffnen einer Gerätebedienung | ADO | M               | M       |

| Feldname | A/F/I/l | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| device   | *       | 003C | Device name<br>type: c-string 1..8                                        |
| devtype  | *       | 003D | Device type<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)          |

## Objekt ANY

| Ereignis                                       | evt | SAT-Information |         |         |       |        |
|------------------------------------------------|-----|-----------------|---------|---------|-------|--------|
|                                                |     | databth         | datahex | datatxt | ldata | subcod |
| ANY event (system exit)<br>beliebiges Ereignis | ANY | O               | O       | O       | E     | O      |

| Feldname | A/F/I/l | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| databth  | *       | 0062 | data type hexa or string<br>type: x-string 2..510                         |
| datahex  | *       | 0061 | data type hexa<br>type: x-string 2..510                                   |
| datatxt  | *       | 0060 | data type text<br>type: c-string 1..510                                   |
| ldata    | *       | 0203 | General hexa fields<br>type: x-string 2..64000                            |
| subcod   | *       | 005F | subcode<br>type: c-string 1..4                                            |

## Objekt APPLICATION

| Ereignis            | evt | res | SAT-Information |         |         |         |         |        |        |    |
|---------------------|-----|-----|-----------------|---------|---------|---------|---------|--------|--------|----|
|                     |     |     | applnam         | hostnam | partnam | pthtnam | parttyp | applid | connid | rc |
| Anwendung öffnen    | DON | S   | M               | O       | -       | -       | -       | M      | -      | M  |
|                     |     | F   | M               | O       | -       | -       | -       | O      | -      | M  |
| Anwendung schließen | DCL | S/F | O               | -       | -       | -       | -       | O      | -      | O  |
| Verbindung aufbauen | DCN | S   | M               | O       | M       | O       | M       | M      | M      | M  |
|                     |     | F   | M               | O       | M       | O       | M       | O      | O      | M  |
| Verbindung abbauen  | DDS | S/F | M               | O       | M       | O       | -       | O      | O      | O  |

| Feldname | A/F/Fl | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter   |
|----------|--------|------|-----------------------------------------------------------------------------|
| applid   | *      | 0035 | Application identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8) |
| applnam  | *      | 0025 | Application name<br>type: c-string 1..8                                     |
| connid   | *      | 0036 | Connection identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)  |
| hostnam  | *      | 0029 | Name of the host<br>type: c-string 1..8                                     |
| partnam  | *      | 0026 | Partner name<br>type: c-string 1..8                                         |
| parttyp  | *      | 0028 | Type of the partner<br>keywords: APPLICATION/TERMINAL                       |
| pthtnam  | *      | 0027 | Name of the partner host<br>type: c-string 1..8                             |
| rc       | *      | 003B | fdbk return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)       |

## Objekt BCAM

| Ereignis           | evt | res | SAT-Information |                      |                      |                      |        |         |         |         |         |         |         |         |                      |                      |                      |         |         |        |    |
|--------------------|-----|-----|-----------------|----------------------|----------------------|----------------------|--------|---------|---------|---------|---------|---------|---------|---------|----------------------|----------------------|----------------------|---------|---------|--------|----|
|                    |     |     | applid          | appliso <sup>1</sup> | applnam <sup>1</sup> | applsoc <sup>1</sup> | connid | hostnam | ipv4own | ipv4ptn | ipv6own | ipv6ptn | itslown | itslptn | partiso <sup>2</sup> | partnam <sup>2</sup> | partsoc <sup>2</sup> | portown | portptn | pthnam | rc |
| TSAP öffnen        | BAO | S   | M               | O                    | O                    | O                    | -      | O       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | O       | -       | -      | M  |
|                    |     | F   | M               | O                    | O                    | O                    | -      | O       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | -       | O       | -      | -  |
| TSAP schließen     | BAC | S   | M               | O                    | O                    | O                    | -      | O       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | O       | -       | -      | M  |
|                    |     | F   | M               | -                    | -                    | -                    | -      | -       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | O       | -       | -      | M  |
| Verbindung öffnen  | BCN | S   | M               | -                    | -                    | -                    | M      | -       | O       | O       | O       | O       | O       | O       | O                    | O                    | O                    | O       | O       | O      | M  |
|                    |     | F   | M               | -                    | -                    | -                    | -      | -       | O       | O       | O       | O       | O       | O       | O                    | O                    | O                    | O       | O       | O      | M  |
| Verbindung beenden | BDS | S   | M               | -                    | -                    | -                    | M      | -       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | -       | -       | -      | M  |
|                    |     | F   | M               | -                    | -                    | -                    | M      | -       | -       | -       | -       | -       | O       | -       | -                    | -                    | -                    | -       | -       | -      | M  |

<sup>1</sup> Die Felder appliso, applnam und applsoc schließen sich gegenseitig aus

<sup>2</sup> Die Felder partiso, partnam und partsoc schließen sich gegenseitig aus

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                 |
|----------|-------|------|-------------------------------------------------------------------------------------------|
| applid   | *     | 0035 | Application identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)               |
| appliso  | *     | 0146 | ISO name of the application<br>type: x-string 156..156 (ALARM/FILTER: x-string 2..156)    |
| applnam  | *     | 0025 | Application name<br>type: c-string 1..8                                                   |
| applsoc  | *     | 0147 | SOCKET name of the application<br>type: x-string 156..156 (ALARM/FILTER: x-string 2..156) |
| connid   | *     | 0036 | Connection identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                |
| hostnam  | *     | 0029 | Name of the host<br>type: c-string 1..8                                                   |
| ipv4own  | *     | 014A | Own IP address (format V4)<br>type: c-string 7..15                                        |
| ipv4ptn  | *     | 014B | Partner IP address (format V4)<br>type: c-string 7..15                                    |
| ipv6own  | *     | 014C | Own IP address (format V6)<br>type: c-string 39..39                                       |
| ipv6ptn  | *     | 014D | Partner IP address (format V6)<br>type: c-string 39..39                                   |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter             |
|----------|---------|------|---------------------------------------------------------------------------------------|
| itslown  | *       | 0151 | Own ISO-TSEL<br>type: x-string 64..64 (ALARM/FILTER: x-string 2..64)                  |
| itslptn  | *       | 0152 | Partner ISO-TSEL<br>type: x-string 64..64 (ALARM/FILTER: x-string 2..64)              |
| partiso  | *       | 0148 | ISO name of the partner<br>type: x-string 156..156 (ALARM/FILTER: x-string 2..156)    |
| partnam  | *       | 0026 | Partner name<br>type: c-string 1..8                                                   |
| partsoc  | *       | 0149 | SOCKET name of the partner<br>type: x-string 156..156 (ALARM/FILTER: x-string 2..156) |
| portown  | *       | 014E | Own port number<br>type: integer 0..65535                                             |
| portptn  | *       | 014F | Partner port number<br>type: integer 0..65535                                         |
| pthtnam  | *       | 0027 | Name of the partner host<br>type: c-string 1..8                                       |
| rc       | *       | 003B | fdbk return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                 |

## Objekt CATALOG

| Ereignis             | evt | res | SAT-Information |       |         |         |        |
|----------------------|-----|-----|-----------------|-------|---------|---------|--------|
|                      |     |     | catid           | share | catacce | resjoin | newcat |
| Katalog importieren  | CIP | S/F | M               | M     | M       | M       | -      |
| Katalog exportieren  | CEP | S/F | M               | -     | -       | -       | -      |
| Katalog prüfen       | CKR | S   | M               | -     | -       | -       | O      |
|                      |     | F   | O               | -     | -       | -       | O      |
| Katalog konvertieren | CVR | S   | M               | -     | -       | -       | M      |
|                      |     | F   | O               | -     | -       | -       | O      |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| catacce  | *     | 0024 | Catalog access status<br>keywords: MASTER/SLAVE                           |
| catid    | *     | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| newcat   | *     | 00EC | new or merged catalog identifier<br>type: c-string 1..4                   |
| resjoin  | *     | 0045 | user-catalog lost or not<br>keywords: YES/NO                              |
| share    | *     | 0023 | Catalog shareability<br>keywords: SHARED/EXCLUSIVE                        |

## Objekt CONSLOG

| Ereignis        | evt              | SAT-Information |          |         |         |        |        |
|-----------------|------------------|-----------------|----------|---------|---------|--------|--------|
|                 |                  | cltype          | clrecept | clsende | clmsgid | cltext | clorig |
| CONSLOG-Eintrag | CLG <sup>1</sup> | M               | M        | -       | M       | M      | M      |
|                 | CLG <sup>2</sup> | M               | M        | M       | -       | M      | M      |
|                 | CLG <sup>3</sup> | M               | -        | M       | -       | M      | M      |

<sup>1</sup> 'System message requiring a response' bis 'Additional information request', siehe unten

<sup>2</sup> 'Response message' und 'Additional information response'

<sup>3</sup> 'Operator command'

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|-------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clmsgid  |       | 0096 | Message id. in Conslog record<br>type: c-string 1..7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| clorig   |       | 0098 | origin of the Conslog record<br>keywords: TPR/TU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| clrecept |       | 0094 | Recipient<br>type: c-string 1..4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| clsende  |       | 0095 | Sender<br>type: c-string 1..4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| cltext   |       | 0097 | Rest of the CONSLOG record<br>type: c-string 1..252                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cltype   |       | 0093 | Type of the CONSLOG record<br>type: c-string 1..39. Possible values:<br>'System message requiring a response' (msg type = ?)<br>'System message not requiring a response' (msg type = %)<br>'Error message' (msg type = *)<br>'Emergency message' (msg type = E)<br>'Command end message' (msg type = !)<br>'Command result' (msg type = +)<br>'Additional information request' (msg type = &)<br>'Response message' (response type = R)<br>'Additional information response' (response type =:)<br>'Operator command' (command type: /) |

## Objekt COOWNER PROTECTION

| Ereignis                                 | evt | SAT-Information |         |        |        |        |         |
|------------------------------------------|-----|-----------------|---------|--------|--------|--------|---------|
|                                          |     | guard           | nwrlnam | objnam | parcra | parcrm | rulenam |
| Regel für Miteigentümerschutz hinzufügen | CRA | M               | -       | -      | E      | -      | M       |
| Regel für Miteigentümerschutz ändern     | CRM | M               | O       | -      | -      | E      | M       |
| Miteigentümerschutzregel anzeigen        | CRQ | -               | -       | M      | -      | -      | -       |
| Regel für Miteigentümerschutz entfernen  | CRR | M               | -       | -      | -      | -      | M       |
| Regel für Miteigentümerschutz anzeigen   | CRS | M               | -       | -      | -      | -      | -       |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| guard    | *     | 009F | Guard name<br>type: c-string 1..40                                        |
| nwrlnam  | *     | 00C1 | New name of protection rule<br>type: c-string 1..12                       |
| objname  | *     | 00C2 | Name of object<br>type: c-string 1..54                                    |
| parcra   | +     | 0215 | Parameter list for add coowner prot rule<br>type: x-string 2..384         |
| parcrm   | +     | 0216 | Parameter list for modify coowner prot rule<br>type: x-string 2..384      |
| rulenam  | *     | 00C0 | Name of protection rule<br>type: c-string 1..20                           |

## Objekt DATA SPACES

| Ereignis                               | evt | res | SAT-Information |      |         |        |         |       |      |   |
|----------------------------------------|-----|-----|-----------------|------|---------|--------|---------|-------|------|---|
|                                        |     |     | acckey          | alet | comread | dsname | mempriv | scope | spid |   |
| DATA SPACE erzeugen                    | DSB | S   | M               | -    | M       | M      | M       | M     | M    | M |
|                                        |     | F   | M               | -    | M       | M      | M       | M     | M    | - |
| mit DATA SPACE verbinden               | DSC | S   | M               | M    | M       | M      | M       | M     | M    | M |
|                                        |     | F   | M               | -    | M       | M      | M       | M     | M    | M |
| Verbindung mit DATA SPACE<br>abbrechen | DSD | S/F | -               | M    | -       | O      | -       | O     | O    | O |
| DATA SPACE löschen                     | DSE | S/F | -               | -    | -       | M      | -       | M     | M    | M |
| DATA SPACE ändern/zurück-<br>setzen    | DSM | S/F | -               | -    | -       | M      | -       | M     | M    | M |

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter         |
|----------|---------|------|-----------------------------------------------------------------------------------|
| acckey   | *       | 0034 | TU access key<br>type: x-string 2..2                                              |
| alet     | *       | 009E | access list entry token<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)      |
| comread  | *       | 009D | read access protection<br>type: keywords: NO/YES                                  |
| dsname   | *       | 009B | data space name<br>type: c-string 1..54                                           |
| mempriv  | *       | 0021 | processed privilege identification<br>keywords: YES/NO                            |
| scope    | *       | 001D | Memory pool scope<br>keywords: LOCAL/GROUP/GLOBAL/USER-GROUP/<br>UNDEFINED/SYSTEM |
| spid     | *       | 009C | Space identifier<br>type: x-string 2..16 (ALARM/FILTER: x-string 16..16)          |

## Objekt DEFAULT PROTECTION

| Ereignis                                    | evt | SAT-Information |         |        |        |        |        |        |        |        |         |
|---------------------------------------------|-----|-----------------|---------|--------|--------|--------|--------|--------|--------|--------|---------|
|                                             |     | guard           | nwrlnam | objnam | pardaa | pardam | pardra | pardrm | pardua | pardur | rulenam |
| Standardwerte für Schutzattribute festlegen | DAA | M               | -       | -      | E      | -      | -      | -      | -      | -      | -       |
| Standardwerte für Schutzattribute ändern    | DAM | M               | -       | -      | -      | E      | -      | -      | -      | -      | -       |
| Standardwerte für Schutzattribute anzeigen  | DAS | M               | -       | -      | -      | -      | -      | -      | -      | -      | -       |
| Regel für Standardschutz hinzufügen         | DRA | M               | -       | -      | -      | -      | E      | -      | -      | -      | M       |
| Regel für Standardschutz ändern             | DRM | M               | O       | -      | -      | -      | -      | E      | -      | -      | M       |
| Standardschutzattribute für Objekt anzeigen | DRQ | -               | -       | M      | -      | -      | -      | -      | -      | -      | -       |
| Regel für Standardschutz entfernen          | DRR | M               | -       | -      | -      | -      | -      | -      | -      | -      | M       |
| Regel für Standardschutz anzeigen           | DRS | M               | -       | -      | -      | -      | -      | -      | -      | -      | -       |
| Benutzerkennung für Objektpfad hinzufügen   | DUA | M               | -       | -      | -      | -      | -      | -      | E      | -      | -       |
| Benutzerkennung für Objektpfad entfernen    | DUR | M               | -       | -      | -      | -      | -      | -      | -      | E      | -       |
| Benutzerkennung für Objektpfad anzeigen     | DUS | M               | -       | -      | -      | -      | -      | -      | -      | -      | -       |

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter  |
|----------|---------|------|----------------------------------------------------------------------------|
| guard    | *       | 009F | Guard name<br>type: c-string 1..40                                         |
| nwrlnam  | *       | 00C1 | New name of protection rule<br>type: c-string 1..12                        |
| objname  | *       | 00C2 | Name of object<br>type: c-string 1..54                                     |
| pardaa   | +       | 020F | Parameter list for add default prot attributes<br>type: x-string 2..312    |
| pardam   | +       | 0210 | Parameter list for modify default prot attributes<br>type: x-string 2..352 |
| pardra   | +       | 0213 | Parameter list for add default prot rule<br>type: x-string 2..424          |
| pardrm   | +       | 0214 | Parameter list for modify default prot rule<br>type: x-string 2..424       |
| pardua   | +       | 0211 | Parameter list for add default prot uid<br>type: x-string 2..952           |
| pardur   | +       | 0212 | Parameter list for remove default prot uid<br>type: x-string 2..952        |
| rulenam  | *       | 00C0 | Name of protection rule<br>type: c-string 1..20                            |

## Objekt EVENTING-ITEM

| Ereignis                      | evt | res    | SAT-Information |        |
|-------------------------------|-----|--------|-----------------|--------|
|                               |     |        | evitnam         | scope  |
| Ereignissteuerung einschalten | EEE | S<br>F | M<br>-          | M<br>- |
| Ereignissteuerung ausschalten | EDE | S<br>F | M<br>-          | M<br>- |
| Serialisierung einschalten    | EES | S<br>F | M<br>-          | M<br>- |
| Serialisierung ausschalten    | EDS | S<br>F | M<br>-          | M<br>- |

| Feldname | A/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                         |
|----------|-------|------|---------------------------------------------------------------------------------------------------|
| evitnam  | *     | 002F | Eventing/serialization item name<br>type: c-string 1..64 (ALARM/FILTER: c-string 64..64)          |
| scope    | *     | 001D | Eventing/serialization item scope<br>keywords: LOCAL/GROUP/GLOBAL/USER-GROUP/<br>UNDEFINED/SYSTEM |

## Objekt FILE

| Ereignis                                       | evt | SAT-Information |         |       |       |                |                |         |                |         |        |      |
|------------------------------------------------|-----|-----------------|---------|-------|-------|----------------|----------------|---------|----------------|---------|--------|------|
|                                                |     | access          | auditat | catid | dmsrc | filename       | fnpatrn        | fparcat | newfile        | pswdpar | sopact | vsn1 |
| Datei erstellen                                | FCD | M <sup>1</sup>  | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei lesen                                    | FRD | M <sup>2</sup>  | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei ausführen (open exec)                    | FED | M               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei modifizieren                             | FMD | M <sup>3</sup>  | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei schließen                                | FCL | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei löschen                                  | FDD | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei mit ARCHIVE umbenennen                   | FAR | -               | M       | -     | O     | M <sup>5</sup> | -              | -       | M <sup>5</sup> | -       | -      | -    |
| Datei umbenennen                               | FRN | -               | M       | -     | O     | M              | -              | -       | M              | -       | -      | -    |
| Schutzattribute erstellen                      | FCS | -               | M       | -     | O     | M              | -              | E       | -              | -       | -      | -    |
| Schutzattribute modifizieren                   | FMS | -               | M       | -     | O     | M              | -              | E       | -              | -       | -      | -    |
| Schutzattribute löschen                        | FDS | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Schutzattribute lesen                          | FRS | -               | M       | O     | -     | O <sup>4</sup> | O <sup>4</sup> | -       | -              | M       | -      | -    |
| Schutzattribute importieren                    | FIS | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Schutzattribute exportieren                    | FES | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei in entschlüsselte Datei umwandeln        | FDC | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| Datei in verschlüsselte Datei umwandeln        | FEC | -               | M       | -     | O     | M              | -              | -       | -              | -       | -      | -    |
| File extents verschieben (SPACEOPT)            | FME | -               | -       | -     | -     | M              | -              | -       | -              | -       | M      | O    |
| Objekt für Reorganisation auswählen (SPACEOPT) | FSO | -               | -       | O     | -     | O              | -              | -       | -              | -       | -      | O    |

<sup>1</sup> nur OUTIN / OUTPUT erlaubt

<sup>2</sup> nur INPUT / REVERSE erlaubt

<sup>3</sup> nur UPDATE / EXTEND / INOUT / SINOUT erlaubt

<sup>4</sup> schließen sich gegenseitig aus

<sup>5</sup> es hängt von der ARCHIVE-Funktion ab, ob die cat-id angegeben wird

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                   |
|----------|---------|------|-------------------------------------------------------------------------------------------------------------|
| access   | *       | 0006 | Open file mode<br>keywords: INPUT/REVERSE/OUTPUT/EXTEND/UPDATE/INOUT/OUTIN/SINOUT/INPUT-EXECUTE/UNSPECIFIED |
| auditat  | *       | 0005 | Audit attribute<br>keywords: SUCCESS/FAILURE/ALL/NONE                                                       |

| <b>Feldname</b> | <b>A/I/Fil</b> | <b>exit</b> | <b>Bedeutung und Werte der Information:<br/>SDF-Datentyp oder Schlüsselwörter</b> |
|-----------------|----------------|-------------|-----------------------------------------------------------------------------------|
| catid           | *              | 0022        | Catalog identifier<br>type: c-string 1..4                                         |
| dmsrc           | *              | 0004        | DMS return code<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)              |
| filename        | *              | 0003        | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                        |
| fnpatrn         | *              | 0063        | filename pattern<br>type: c-string 1..80                                          |
| fparcat         | +              | 0208        | Parameter List File<br>Type: x-string 2..12000                                    |
| newfile         | *              | 0007        | New file name<br>type: c-string 1..54 (ALARM/FILTER: filename)                    |
| pswdpar         | *              | 0064        | password parameter<br>keywords: YES/NO                                            |
| sopact          | *              | 0065        | SPACEOPT action code<br>keywords: CLEAR-VOL/REDUCE-EXT/<br>START-JOB              |
| vsn1            | *              | 0039        | Volume serial number<br>type: c-string 1..6                                       |

**Objekt FITC (Fast Intertask Communication)**

| Ereignis                      | evt | SAT-Information |      |         |
|-------------------------------|-----|-----------------|------|---------|
|                               |     | guard           | port | tsn-inf |
| Port Access definieren        | POA | M               | M    | O       |
| Port definieren               | POB | M               | M    | O       |
| an Port anschließen           | POC | M               | M    | O       |
| von Port trennen              | POD | M               | M    | O       |
| Port freigeben                | POE | M               | M    | O       |
| Port Access freigeben         | POR | M               | M    | O       |
| impliziter Austausch mit Port | POX | M               | M    | O       |

| Feldname | A/F/i | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| guard    | *     | 009F | Guard name<br>type: c-string 1..40                                        |
| port     | *     | 00B0 | port name<br>type: c-string 1..54                                         |
| tsn-inf  | *     | 0010 | TSN object<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)           |

## Objekt GROUP

| Ereignis     | evt | SAT-Information |       |         |         |         |       |
|--------------|-----|-----------------|-------|---------|---------|---------|-------|
|              |     | admin           | catid | gparadu | gparmdu | obj-gid | upper |
| hinzufügen   | GAD | M               | M     | E       | -       | M       | M     |
| modifizieren | GMD | O               | M     | -       | E       | M       | O     |
| entfernen    | GRM | M               | M     | -       | -       | M       | M     |
| anzeigen     | GSH | -               | M     | -       | -       | M       | -     |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| admin    | *     | 002B | (Group)administrator identification<br>type: c-string 1..8 (user-id)      |
| catid    | *     | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| gparadu  | +     | 0209 | Parameter list for add group<br>type: x-string 2..5000                    |
| gparmdu  | +     | 0210 | Parameter list for modify group<br>type: x-string 2..10000                |
| obj-gid  | *     | 002A | Group identifier as object<br>type: c-string 1..8                         |
| upper    | *     | 002C | Upper group identification<br>type: c-string 1..8                         |

## Objekt GUARDS

| Ereignis                     | evt | SAT-Information |         |         |       |         |
|------------------------------|-----|-----------------|---------|---------|-------|---------|
|                              |     | catid           | gparmod | gparrem | guard | nwguard |
| Guard erzeugen               | GUB | -               | -       | -       | M     | -       |
| Guard kopieren               | GUC | -               | -       | -       | M     | M       |
| Guard löschen                | GUD | -               | -       | -       | M     | -       |
| Guardskatalog wechseln       | GUF | M               | -       | -       | -     | -       |
| Guardskatalog reparieren     | GUR | M               | -       | -       | -     | -       |
| Attribute ändern             | GUM | -               | -       | -       | M     | O       |
| Attribute anzeigen           | GUS | -               | -       | -       | M     | -       |
| Zugriffsbedingung definieren | GAA | -               | E       | -       | M     | -       |
| Zugriffsbedingung ändern     | GAM | -               | E       | -       | M     | -       |
| Zugriffsbedingung löschen    | GAR | -               | -       | E       | M     | -       |
| Zugriffsbedingung anzeigen   | GAS | -               | -       | -       | M     | -       |
| Zugriffsbedingung abfragen   | GAQ | -               | -       | -       | M     | -       |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| catid    | *     | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| gparmod  | +     | 0201 | Modify parameter list<br>type: x-string 2..1860                           |
| gparrem  | +     | 0202 | delete parameter list<br>type: x-string 2..432                            |
| guard    | *     | 009F | Guard name<br>type: c-string 1..40                                        |
| nwguard  | *     | 00AB | new guard name<br>type: c-string 1..24                                    |

## Objekt IPSEC

| Ereignis                                             | evt | res            | SAT-Information      |                      |                      |                      |    |
|------------------------------------------------------|-----|----------------|----------------------|----------------------|----------------------|----------------------|----|
|                                                      |     |                | ipv4own <sup>1</sup> | ipv4ptn <sup>2</sup> | ipv6own <sup>1</sup> | ipv6ptn <sup>2</sup> | rc |
| IPSEC Security Datenbasis laden                      | ILD | S<br>F         | -                    | -                    | -                    | -                    | -  |
| Verstoß gegen die Security Policy beim Datentransfer | IPV | F <sup>3</sup> | O                    | O                    | O                    | O                    | M  |

<sup>1</sup> Die Felder ipv4own und ipv6own schließen sich gegenseitig aus.

<sup>2</sup> Die Felder ipv4ptn und ipv6ptn schließen sich gegenseitig aus.

<sup>3</sup> Beim Ereignis IPV ist das Resultat immer F

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|--------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv4own  | *      | 014A | Own IP address (format V4)<br>type: c-string 7..15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ipv4ptn  | *      | 014B | Partner IP address (format V4)<br>type: c-string 7..15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ipv6own  | *      | 014C | Own IP address (format V6)<br>type: c-string 39..39                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ipv6ptn  | *      | 014D | Partner IP address (format V6)<br>type: c-string 39..39                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rc       | *      | 003B | fdbk return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)<br>Folgende Returncodes sind auswertbar: <ul style="list-style-type: none"> <li>- X'00400106' unzulässiger Wert für SPI (Security Parameter Index)</li> <li>- X'00400206' ungültige Signatur</li> <li>- X'00400306' Fehlermeldung der Cryptobox: Entschlüsselung schlug fehl</li> <li>- X'00400406' Signatur/Verschlüsselung erforderlich</li> <li>- X'00400506' 1. Security Association für Input erforderlich, aber nicht verfügbar</li> <li>- X'00400606' 2. Security Association für Input erforderlich, aber nicht verfügbar</li> <li>- X'00400706' Unzulässiger Security Protokoll-Header</li> </ul> |

## Objekt JOB

| Ereignis                              | evt | res | SAT-Information |         |         |       |        |         |         |         |       |        |       |         |         |
|---------------------------------------|-----|-----|-----------------|---------|---------|-------|--------|---------|---------|---------|-------|--------|-------|---------|---------|
|                                       |     |     | calend          | endreas | endtype | flush | intime | jobtype | obj-uid | procnam | rejas | repeat | rerun | station | tsn-inf |
| Stapelauftrag oder Subtask einleiten  | JBE | S   | M               | -       | -       | M     | -      | M       | M       | -       | -     | M      | M     | -       | M       |
| Auftrag abbrechen                     | JCN | S   | -               | O       | -       | -     | -      | -       | O       | -       | M     | -      | -     | -       | -       |
| Dialog oder RLOGIN einleiten          | JDE | S   | -               | -       | -       | -     | -      | -       | -       | M       | -     | -      | -     | M       | -       |
| Auftrag beenden                       | JED | S   | -               | M       | M       | -     | -      | -       | O       | M       | M     | -      | -     | M       | -       |
| Stapelauftrag oder Subtask initiieren | JIN | S   | -               | -       | -       | -     | M      | -       | -       | -       | -     | -      | -     | -       | M       |
| Stapelauftrag modifizieren            | JMD | S   | M               | -       | -       | M     | -      | -       | -       | -       | -     | M      | M     | -       | M       |
| POSIX-Task erzeugen                   | JFK | S   | -               | -       | -       | -     | -      | -       | -       | -       | -     | -      | -     | -       | M       |
|                                       |     | F   | -               | -       | -       | -     | -      | -       | -       | -       | -     | -      | -     | -       | O       |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                  |
|----------|---------|------|--------------------------------------------------------------------------------------------|
| calend   | *       | 00F0 | calendar date for job-start<br>keywords: YES/NO                                            |
| endreas  | *       | 0017 | End reason<br>keywords: ABEND/CANCEL/LOGOFF/MOVE-JOBS/SHUTDOWN                             |
| endtype  | *       | 0016 | Job termination status<br>keywords: NORMAL/ABNORMAL                                        |
| flush    | *       | 0014 | Job removal<br>keywords: YES/NO                                                            |
| intime   | *       | 001A | Time of the job spoolin<br>type: c-string 1..14 (ALARM/FILTER: c-string 14..14)            |
| jobtype  | *       | 0012 | Job type<br>keywords: ENTR = ENTER job, TASK = subtask, MOVE-JOBS = import job description |
| obj-uid  | *       | 0011 | user identificator as object<br>type: c-string 1..8                                        |
| procnam  | *       | 0019 | Processor name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                        |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                         |
|----------|---------|------|---------------------------------------------------------------------------------------------------|
| rejreas  | *       | 001B | Reject reason<br>keywords: INV-AUTHORIZATION/SYSTEM-ERROR/<br>CMD-PARAM-ERROR/SATURATION/NO-ERROR |
| repeat   | *       | 0015 | Job start period<br>keywords: YES/NO                                                              |
| rerun    | *       | 0013 | Job reinitiation<br>keywords: YES/NO                                                              |
| station  | *       | 0018 | Terminal name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                |
| tsn-inf  | *       | 0010 | TSN object<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)                                   |

### Objekt JOB VARIABLES

| Ereignis                     | evt | SAT-Information |         |       |       |
|------------------------------|-----|-----------------|---------|-------|-------|
|                              |     | jvname          | jvpatrn | jvsrc | newjv |
| umbenennen mit ARCHIVE       | JVA | M               | -       | O     | M     |
| Schutzattribute erstellen    | JVC | M               | -       | O     | -     |
| Schutzattribute löschen      | JVD | M               | -       | O     | -     |
| Schutzattribute modifizieren | JVM | M               | -       | O     | -     |
| Daten lesen (GETJV)          | JVG | M               | -       | O     | -     |
| Daten schreiben (SETJV)      | JVS | M               | -       | O     | -     |
| JV abfragen                  | JVQ | O*              | O*      | O     | -     |
| JV umbenennen                | JVR | M               | -       | O     | M     |

\* schließen sich gegenseitig aus

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter   |
|----------|---------|------|-----------------------------------------------------------------------------|
| jvname   | *       | 005B | Job variable-name<br>type: c-string 1..54 (ALARM/FILTER: filename)          |
| jvpatrn  | *       | 005E | Job variable-pattern<br>type: c-string 1..80                                |
| jvsrc    | *       | 005D | Return-code of job variables<br>x-string 2..4 (ALARM/FILTER: x-string 4..4) |
| newjv    | *       | 005C | New job variable name<br>type: c-string 1..54 (ALARM/FILTER: filename)      |

## Objekt KEY

| Ereignis                                                                                                          | evt              | SAT-Information |         |      |         |         |          |         |
|-------------------------------------------------------------------------------------------------------------------|------------------|-----------------|---------|------|---------|---------|----------|---------|
|                                                                                                                   |                  | catid           | enctype | kvno | obj-uid | parkrbp | princccl | princsv |
| KERBEROS Verschlüsselungstyp hinzufügen                                                                           | KEA              | M               | M       | M    | -       | -       | -        | M       |
| KERBEROS Verschlüsselungstyp löschen                                                                              | KED              | M               | M       | M    | -       | -       | -        | M       |
| KERBEROS Principal hinzufügen                                                                                     | KPA              | M               | -       | -    | -       | E       | -        | M       |
| KERBEROS Principal löschen                                                                                        | KPD              | M               | -       | -    | -       | -       | -        | M       |
| KERBEROS Principal ändern                                                                                         | KPM              | M               | -       | -    | -       | E       | -        | M       |
| KERBEROS Ticket prüfen                                                                                            | KTC <sup>1</sup> | -               | M       | M    | O       | -       | M        | M       |
| Fehlversuch bei der Crypto-Kennwort-Überprüfung nach Überschreitung der maximal erlaubten Anzahl an Fehlversuchen | KXM <sup>2</sup> | -               | -       | -    | -       | -       | -        | -       |

<sup>1</sup> Beim Ereignis KTC ist das Datenfeld user-id ohne Bedeutung.

Bei Dialog-Logon ist das Feld nicht versorgt. Bei Zugang über eine Anwendung wie z.B.OMNIS oder UTM enthält es die Benutzererkennung des Aufrufers, nicht jedoch die Ziel-Benutzererkennung.

<sup>2</sup> Beim Ereignis KXM kann das das Resultat 'S' nicht auftreten; das Resultat ist also immer 'F'

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                             |
|----------|---------|------|-------------------------------------------------------------------------------------------------------|
| catid    | *       | 0022 | Catalog identifier<br>type: c-string 1..4                                                             |
| enctype  | *       | 0174 | KERBEROS encryption type<br>type: integer 0..2 <sup>31</sup> -1                                       |
| kvno     | *       | 0175 | KERBEROS key version number<br>type: integer 0..2 <sup>31</sup> -1                                    |
| obj-uid  | *       | 0011 | User identifier as object<br>type: c-string 1..8                                                      |
| parkrbp  | +       | 0219 | Parameter list for add/modify KERBEROS principal<br>type: x-string 2..280                             |
| princccl | *       | 0172 | KERBEROS client principal<br>type: c-string 1..1800 with-low (ALARM/FILTER: c-string 1..255 with-low) |
| princsv  | *       | 0173 | KERBEROS server principal<br>type: c-string 1..1800 with-low (ALARM/FILTER: c-string 1..255 with-low) |

## Objekt MEMORY-POOL

| Ereignis                                       | evt | res | SAT-Information |       |         |         |         |         |        |
|------------------------------------------------|-----|-----|-----------------|-------|---------|---------|---------|---------|--------|
|                                                |     |     | mempool         | scope | memclas | mempriv | enamprc | shortid | acckey |
| eröffnen (ENAMP)                               | MEN | S   | M               | M     | M       | M       | M       | M       | M      |
|                                                |     | F   | M               | O     | O       | O       | M       | -       | O      |
| schließen (DISMP)                              | MDS | S/F | M               | M     | -       | -       | -       | -       | -      |
| freigeben (RELMP)                              | MRL | S/F | M               | M     | -       | -       | -       | -       | -      |
| lesbar machen für TU<br>(mit (\$)CSTMP in TPR) | MRD | S/F | M               | M     | -       | -       | -       | -       | -      |
| Lesbarkeit ändern mit<br>CSTMP in TU           | MAC | S/F | M               | M     | -       | -       | -       | -       | -      |

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter         |
|----------|---------|------|-----------------------------------------------------------------------------------|
| acckey   | *       | 0034 | TU access key<br>type: x-string 2..2                                              |
| enamprc  | *       | 001E | ENAMP return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)            |
| memclas  | *       | 0020 | memory class of the memory pool<br>keywords: CLASS5/CLASS6                        |
| mempool  | *       | 001C | memory pool name<br>type: c-string 1..54                                          |
| mempriv  | *       | 0021 | Privilege of the mem. pool pages<br>keywords: YES/NO                              |
| scope    | *       | 001D | Memory pool scope<br>keywords: LOCAL/GROUP/GLOBAL/USER-GROUP/<br>UNDEFINED/SYSTEM |
| shortid  | *       | 001F | Short memory pool name<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)       |

## Objekt OPERATOR-ROLES

| Ereignis                                 | evt | SAT-Information |         |        |         |
|------------------------------------------|-----|-----------------|---------|--------|---------|
|                                          |     | catid           | obj-uid | oprole | routcod |
| Routing Code hinzufügen                  | ORA | M               | -       | M      | M       |
| Operator Role erzeugen                   | ORB | M               | -       | M      | -       |
| Operator Role zuweisen                   | ORC | M               | M       | M      | -       |
| Operator Role aus Benutzersatz entfernen | ORD | M               | M       | M      | -       |
| Operator Role löschen                    | ORE | M               | -       | M      | -       |
| Routing-Code entziehen                   | ORR | M               | -       | M      | M       |

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| catid    | *       | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| obj-uid  | *       | 0011 | User identifier as object<br>type: c-string 1..8                          |
| oprole   | *       | 00AE | operator role<br>type: c-string 1..8                                      |
| routcod  | *       | 00AD | routing code<br>type: c-string 1..3                                       |

## Objekt PLAM-Elemente

| Ereignis                        | evt | res | SAT-Information |         |         |         |         |         |         |        |         |         |
|---------------------------------|-----|-----|-----------------|---------|---------|---------|---------|---------|---------|--------|---------|---------|
|                                 |     |     | filename        | eltname | eltvers | elttype | nwelnam | nwelver | nweltyp | plamrc | keepopt | auditat |
| Bibliothekselement erstellen    | LCE | S   | M               | M       | M       | M       | O       | O       | O       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | O       | O       | M      | -       | M       |
| Bibliothekselement modifizieren | LME | S   | M               | M       | M       | M       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Bibliothekselement lesen        | LRE | S   | M               | M       | M       | M       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Bibliothekselement ausführen    | LEE | S   | M               | M       | M       | M       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Bibliothekselement schließen    | LCL | S   | M               | M       | M       | M       | -       | -       | -       | -      | M       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | M       |
| Bibliothekselement löschen      | LDE | S   | M               | M       | M       | M       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Bibliothekselement umbenennen   | LRN | S   | M               | M       | M       | M       | M       | M       | M       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | M       | M       | M      | M       | -       |
| Sicherheitsattribut erzeugen    | LCS | S   | M               | O       | O       | O       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Sicherheitsattribut löschen     | LDS | S   | M               | O       | O       | O       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |
| Sicherheitsattribut verändern   | LMS | S   | M               | O       | O       | O       | -       | -       | -       | -      | -       | M       |
|                                 |     |     | F               | M       | O       | O       | O       | -       | -       | -      | M       | -       |

| Feldname | A/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| auditat  | *     | 0005 | Audit attribute<br>keywords: SUCCESS/FAILURE/ALL/NONE                     |
| eltname  | *     | 0008 | Element name<br>type: c-string 1..64                                      |
| elttype  | *     | 000A | Element type<br>type: c-string 1..8                                       |
| eltvers  | *     | 0009 | Element version<br>type: c-string 1..24                                   |
| filename | *     | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |
| keepopt  | *     | 0047 | Keep option<br>keywords: YES/NO                                           |

| Feldname | A/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                            |
|----------|-------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nwelnam  | *     | 0042 | New/base element name<br>type: c-string 1..64                                                                                                                                                                                                                        |
| nweltyp  | *     | 0044 | New/base element type<br>type: c-string 1..8                                                                                                                                                                                                                         |
| nwelver  | *     | 0043 | New/base element version<br>type: c-string 1..24                                                                                                                                                                                                                     |
| plamrc   | *     | 0046 | PLAM return code<br>type: c-string 1..13 (ALARM/FILTER: x-string 16..16).<br>Format: zzzz/xxxxxxx<br>zzzz = Primärkode (Dezimal)<br>xxxxxxx= Sekundärkode (Sedezimal)<br>Mit /HELP PLAzxxx kann Information über den entsprechenden Return-<br>code abgerufen werden |

## Objekt POSIX-CHILD-Process

| Ereignis                                         | evt | res | SAT-Information |         |         |       |     |        |
|--------------------------------------------------|-----|-----|-----------------|---------|---------|-------|-----|--------|
|                                                  |     |     | curpid          | curruid | curruid | errno | pid | retval |
| Neuen Prozess erzeugen (fork)                    | XFK | S   | M               | M       | M       | M     | M   | M      |
|                                                  |     | F   | M               | M       | M       | M     | O   | M      |
| Neuen Prozess bei rlogin-Zugang erzeugen (rfork) | XRF | S   | M               | M       | M       | M     | M   | M      |
|                                                  |     | F   | M               | M       | M       | M     | O   | M      |

| Feldname | A/I/F/i | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                 |
|----------|---------|------|-------------------------------------------------------------------------------------------|
| curpid   | *       | 0100 | Current process id of the calling process<br>type: integer 0..2 <sup>31</sup> -1          |
| curruid  | *       | 0102 | Current real POSIX group id of the calling process<br>type: integer 0..2 <sup>31</sup> -1 |
| curruid  | *       | 0101 | Current real POSIX user id of the calling process<br>type: integer 0..2 <sup>31</sup> -1  |
| errno    | *       | 0103 | POSIX error number<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                 |
| pid      | *       | 010F | Process id<br>type: integer 0..2 <sup>31</sup> -1                                         |
| retval   | *       | 0104 | POSIX return value<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                 |

## Objekt POSIX-FILE-and-Directory

| Ereignis                                                                | evt | res | SAT-Information |         |        |        |        |         |        |         |         |         |         |       |    |
|-------------------------------------------------------------------------|-----|-----|-----------------|---------|--------|--------|--------|---------|--------|---------|---------|---------|---------|-------|----|
|                                                                         |     |     | accgrp          | accmode | acooth | accusr | atflag | cloexec | curpid | currgid | curruid | dirdes1 | dirdes2 | errno | .. |
| Aktuelles Dateiverzeichnis wechseln (chdir)                             | XCD | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Datei schließen (close)                                                 | XCL | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateizugriffsrechte ändern (chmod)                                      | XCM | S   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Eigentümer oder Gruppe einer Datei ändern (chown)                       | XCO | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Neue Datei erzeugen (create)                                            | XCR | S   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Verzeichnis via Deskriptor erzeugen (mkdirat)                           | XDA | S   | M               | -       | M      | M      | -      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                         |     | F   | M               | -       | M      | M      | -      | -       | M      | M       | M       | M       | -       | M     |    |
| Dateideskriptor duplizieren (dup)                                       | XDP | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Kontrolloperation auf Dateien (fcntl)                                   | XFC | S   | -               | O       | -      | -      | -      | O       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | O       | -      | -      | -      | O       | M      | M       | M       | -       | -       | M     |    |
| Aktuelles Dateiverzeichnis via Deskriptor wechseln (fchdir)             | XFD | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateizugriffsrechte ändern via Deskriptor (fchmod)                      | XFM | S   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | M               | -       | M      | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Eigentümer oder Gruppe einer Datei via Deskriptor ändern (fchown)       | XFO | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Link zu einer Datei via Deskriptor erzeugen (linkat)                    | XLA | S   | -               | -       | -      | -      | M      | -       | M      | M       | M       | M       | M       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | M      | -       | M      | M       | M       | M       | M       | M     |    |
| Verweis auf eine Datei erzeugen (link)                                  | XLN | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Eigentümer oder Gruppe einer Datei oder eines Verweises ändern (lchown) | XLO | S   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                         |     | F   | -               | -       | -      | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |

Ereignis XCD - XLO (Teil 1)

| evt | res | SAT-Information |        |         |        |          |        |         |        |     |         |         |        |         |         |         |         |         |        |         |         |        |        |     |
|-----|-----|-----------------|--------|---------|--------|----------|--------|---------|--------|-----|---------|---------|--------|---------|---------|---------|---------|---------|--------|---------|---------|--------|--------|-----|
|     |     | fappend         | fcreat | ftclcmd | ftides | filename | filpos | fnoctty | ftrunc | gid | linknam | mapaddr | maplen | mapprot | mapshar | newfdes | newpath | pathnam | retval | sdevrdo | setsgid | setuid | symdev | uid |
| XCD | S   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XCL | S   | -               | -      | -       | -      | M        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XCM | S   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | M       | M      | -      | -   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | M       | M      | -      | -   |
| XCO | S   | -               | -      | -       | -      | -        | -      | -       | -      | M   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -      | -      | M   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | M      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | M   |
| XCR | S   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | M       | M      | -      | -   |
|     | F   | -               | -      | -       | O      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | M       | M      | -      | -   |
| XDA | S   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | M       | M      | -      | -   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | M       | M      | -      | -   |
| XDP | S   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | M       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | O       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XFC | S   | O               | O      | M       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | O               | O      | M       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | O       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XFD | S   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XFM | S   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | M       | M      | -      | -   |
|     | F   | -               | -      | -       | M      | -        | -      | -       | -      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | M       | M      | -      | -   |
| XFO | S   | -               | -      | -       | M      | -        | -      | -       | -      | M   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | M   |
|     | F   | -               | -      | -       | M      | -        | -      | -       | -      | M   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | M   |
| XLA | S   | -               | -      | -       | -      | -        | -      | -       | -      | -   | M       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | -      | -   | O       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XLN | S   | -               | -      | -       | -      | -        | -      | -       | -      | -   | M       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | -      | -   | O       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | -   |
| XLO | S   | -               | -      | -       | -      | -        | -      | -       | -      | M   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | M   |
|     | F   | -               | -      | -       | -      | -        | -      | -       | M      | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -      | -      | M   |

Ereignis XCD - XLO (Teil 2)

| Ereignis                                                                     | evt | res | SAT-Information |         |       |        |        |         |        |         |         |         |         |       |    |
|------------------------------------------------------------------------------|-----|-----|-----------------|---------|-------|--------|--------|---------|--------|---------|---------|---------|---------|-------|----|
|                                                                              |     |     | accgrp          | accmode | accth | accusr | afflag | cloexec | curpid | currgid | curruid | dirdes1 | dirdes2 | errno | .. |
| Dateizugriffsrechte via Deskriptor ändern (fchmodat)                         | XMA | S   | M               | -       | M     | M      | M      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                              |     | F   | M               | -       | M     | M      | M      | -       | M      | M       | M       | M       | -       | M     |    |
| Dateiverzeichnis erzeugen (mkdir)                                            | XMD | S   | M               | -       | M     | M      | -      | --      | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | M               | -       | M     | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Abbildung Datei in virtuellen Speicher (mmap)                                | XMM | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Schutzattribute für Abbildung Datei in virtuellen Speicher setzen (mprotect) | XMP | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateisystem einhängen (mount)                                                | XMT | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Abbildung Datei in virtuellen Speicher aufheben (munmap)                     | XMU | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Datei via Deskriptor öffnen (openat)                                         | XOA | S   | O               | M       | O     | O      | -      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                              |     | F   | O               | M       | O     | O      | -      | -       | M      | M       | M       | M       | -       | M     |    |
| Datei öffnen (open)                                                          | XOP | S   | O               | M       | O     | O      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | O               | M       | O     | O      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateiname via Deskriptor ändern (renameat)                                   | XRA | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | M       | M       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | M       | M       | M     |    |
| Dateiverzeichnis löschen (rmdir)                                             | XRD | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateiname ändern (rename)                                                    | XRN | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Symbolischen Verweis auf eine Datei via Deskriptor erzeugen (symlinkat)      | XSA | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | M       | -       | M     |    |
| Symbolischen Verweis auf eine Datei erzeugen (symlink)                       | XSL | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Datei oder Verzeichnis via Deskriptor löschen (unlinkat)                     | XUA | S   | -               | -       | -     | -      | M      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | M      | -       | M      | M       | M       | M       | -       | M     |    |
| Dateibitmaske für einen Prozess setzen (umask)                               | XUM | S   | M               | -       | M     | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | M               | -       | M     | M      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Datei löschen (remove/unlink)                                                | XUN | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Dateisystem aushängen (umount)                                               | XUT | S   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | -      | -       | M      | M       | M       | -       | -       | M     |    |
| Gruppe oder Besitzer einer Datei via Deskriptor ändern (fchownat)            | XWA | S   | -               | -       | -     | -      | M      | -       | M      | M       | M       | M       | -       | M     |    |
|                                                                              |     | F   | -               | -       | -     | -      | M      | -       | M      | M       | M       | M       | -       | M     |    |

Ereignis XMA - XWA (Teil 1)

| evt | res | SAT-Information |        |        |       |          |        |         |       |     |         |         |        |         |         |         |         |         |        |         |         |         |         |     |
|-----|-----|-----------------|--------|--------|-------|----------|--------|---------|-------|-----|---------|---------|--------|---------|---------|---------|---------|---------|--------|---------|---------|---------|---------|-----|
|     |     | fappend         | fcreat | fctcmd | files | filename | filpos | fnoctty | frunc | gid | linknam | mapaddr | maplen | mapprot | mapshar | newfdes | newpath | pathnam | retval | sdevrdo | setsgid | setsuid | symbdev | uid |
| XMA | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | -       | -      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | -       | -      | -       | -       | -       | -       | -   |
| XMD | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | M       | M      | -       | M       | M       | M       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | M       | M      | -       | M       | M       | M       | -   |
| XMM | S   | -               | -      | -      | M     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | O       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | M     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | O       | M      | -       | -       | -       | -       | -   |
| XMP | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | -       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | M       | M       | -       | -       | -       | M      | -       | -       | -       | -       | -   |
| XMT | S   | -               | -      | -      | -     | O        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | M       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | O        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | M       | -       | -       | -       | -   |
| XMU | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | -       | -       | -       | -       | -       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | M       | M      | -       | -       | -       | -       | -       | M      | -       | -       | -       | -       | -   |
| XOA | S   | M               | M      | -      | M     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | O       | O       | O       | -   |
|     | F   | M               | M      | -      | O     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | O       | O       | O       | -   |
| XOP | S   | M               | M      | -      | O     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | O       | O       | O       | -   |
|     | F   | M               | M      | -      | O     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | O       | O       | O       | -   |
| XRA | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XRD | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XRN | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XSA | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | M       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | O       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XSL | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | M       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | O       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XUA | S   | M               | -      | -      | -     | -        | -      | -       | -     | -   | M       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | M               | -      | -      | -     | -        | -      | -       | -     | -   | O       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XUM | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | M       | M       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | M       | M       | -       | -   |
| XUN | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | M       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | O       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XUT | S   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | -     | -   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
| XWA | S   | -               | -      | -      | -     | -        | -      | -       | -     | M   | -       | -       | -      | -       | -       | -       | -       | M       | M      | -       | -       | -       | -       | -   |
|     | F   | -               | -      | -      | -     | -        | -      | -       | M     | M   | -       | -       | -      | -       | -       | -       | -       | O       | M      | -       | -       | -       | -       | M   |

Ereignis XMA - XWA (Teil 2)

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                 |
|----------|---------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accgrp   | *       | 0127 | Access rights for the group<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                                                                                                                                                          |
| accmode  | *       | 0125 | Access mode<br>keywords: READ/READ-AND-WRITE/WRITE/SEARCH                                                                                                                                                                 |
| accth    | *       | 0128 | Access rights for other users<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                                                                                                                                                        |
| accusr   | *       | 0126 | Access rights for the owner<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                                                                                                                                                          |
| atflag   | *       | 0179 | Flag for file operations/events<br>keywords: NONE/<br>AT-SYMLINK-NOFOLLOW ( <i>in case of event XMA or XWA</i> ) /<br>AT-SYMLINK-FOLLOW ( <i>in case of event XLA</i> ) /<br>AT-REMOVEDIR ( <i>in case of event XUA</i> ) |
| cloexec  | *       | 013A | Close file on exec<br>keywords: NO/YES                                                                                                                                                                                    |
| curpid   | *       | 0100 | Current process id of the calling process<br>type: integer 0.. $2^{31}-1$                                                                                                                                                 |
| currgid  | *       | 0102 | Current real POSIX group id of the calling process<br>type: integer 0.. $2^{31}-1$                                                                                                                                        |
| curruid  | *       | 0101 | Current real POSIX user id of the calling process<br>type: integer 0.. $2^{31}-1$                                                                                                                                         |
| dirdes1  | *       | 0177 | File descriptor for the first directory<br>type: integer 0.. $2^{31}-1$                                                                                                                                                   |
| dirdes2  | *       | 0178 | File descriptor for the second directory<br>type: integer 0.. $2^{31}-1$                                                                                                                                                  |
| errno    | *       | 0103 | POSIX error number<br>type: integer $-2^{31}$ .. $2^{31}-1$                                                                                                                                                               |
| fappend  | *       | 0136 | Append to the end of file<br>keywords: NO/YES                                                                                                                                                                             |
| fcreat   | *       | 0137 | Create file<br>keywords: NO/YES                                                                                                                                                                                           |
| fctlcmd  | *       | 012D | File control operation<br>keywords: DUP-FILDES/SET-FILDES-FLAGS/<br>SET-FILMODE-FLAGS                                                                                                                                     |
| fildes   | *       | 010C | File descriptor<br>type: integer 0.. $2^{31}-1$                                                                                                                                                                           |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                    |
|----------|---------|------|--------------------------------------------------------------------------------------------------------------|
| filename | *       | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                                   |
| filpos   | *       | 011B | Offset in mapped file (in multiple of 512)<br>type: integer 0..2 <sup>31</sup> -1                            |
| fnoctty  | *       | 0139 | No controlling terminal<br>keywords: NO/YES                                                                  |
| frunc    | *       | 0138 | Truncate file length to 0<br>keywords: NO/YES                                                                |
| gid      | *       | 0114 | POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                                                        |
| linknam  | *       | 0107 | Link name<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)                        |
| mapaddr  | *       | 011C | Memory address of the mapping<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                           |
| maplen   | *       | 011D | Length of the mapped area<br>type: integer 0..2 <sup>31</sup> -1                                             |
| mapprot  | *       | 0129 | Access permission for the mapped pages<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                                  |
| mapshar  | *       | 012A | Visibility of write accesses to the mapped pages<br>keywords: PRIVATE/SHARED                                 |
| newfdes  | *       | 010D | New file descriptor<br>type: integer 0..2 <sup>31</sup> -1                                                   |
| newpath  | *       | 0106 | New name of file resp. directory<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255) |
| pathnam  | *       | 0105 | Name of file resp. directory<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)     |
| retval   | *       | 0104 | POSIX return value<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                                    |
| sdevrdo  | *       | 013D | Symbolic device is read only<br>keywords: NO/YES                                                             |
| setsgid  | *       | 013C | Set the set-group-id bit<br>keywords: NO/YES                                                                 |
| setsuid  | *       | 013B | Set the set-user-id bit<br>keywords: NO/YES                                                                  |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                      |
|----------|---------|------|----------------------------------------------------------------------------------------------------------------|
| symbdev  | *       | 010A | Symbolic device name (/dev/disk/nxxx)<br>type: c-string 1..14 with-low<br>(ALARM/FILTER: posix-pathname 1..14) |
| uid      | *       | 0111 | POSIX user id<br>type: integer 0..2 <sup>31</sup> -1                                                           |

## Objekt POSIX-PROCESS

| Ereignis                                                                         | evt              | res    | SAT-Information |         |        |          |         |      |       |      |     |        |         |         |      |     |         |         |        |      |      |         |        |     |
|----------------------------------------------------------------------------------|------------------|--------|-----------------|---------|--------|----------|---------|------|-------|------|-----|--------|---------|---------|------|-----|---------|---------|--------|------|------|---------|--------|-----|
|                                                                                  |                  |        | curlim          | curlim2 | curpid | curregid | curruid | egid | errno | euid | gid | maxlim | maxlim2 | pathnam | pgid | pid | pidrecv | resourc | retval | rgid | ruid | setpcmd | signal | uid |
| Effektive Gruppennummer eines Prozesses setzen (setegid)                         | XEG              | S/F    | -               | -       | M      | M        | M       | M    | M     | -    | -   | -      | -       | -       | -    | -   | -       | M       | -      | -    | -    | -       | -      | -   |
| Effektive Benutzernummer eines Prozesses setzen (seteuid)                        | XEU              | S/F    | -               | -       | M      | M        | M       | -    | M     | M    | -   | -      | -       | -       | -    | -   | -       | M       | -      | -    | -    | -       | -      | -   |
| Datei ausführen (exec)                                                           | XEX              | S<br>F | -               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | M       | -    | -   | -       | M       | -      | -    | -    | -       | -      | -   |
| Maximalmenge von Gruppenmitgliedschaften für einen Prozess festlegen (setgroups) | XGR              | S/F    | -               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | O       | -    | -   | -       | M       | -      | -    | -    | -       | -      | -   |
| Signal an Prozess oder Prozessgruppe senden (kill)                               | XKL              | S/F    | -               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | -       | -    | M   | -       | M       | -      | -    | -    | M       | -      | -   |
| Prozessgrenzen setzen (ulimit)                                                   | XLM              | S/F    | M               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | -       | -    | -   | -       | M       | -      | -    | -    | -       | -      | M   |
| Reale und effektive Gruppennummer eines Prozesses setzen (setregid)              | XRG              | S/F    | -               | -       | M      | M        | M       | M    | M     | -    | -   | -      | -       | -       | -    | -   | -       | M       | M      | -    | -    | -       | -      | -   |
| Reale und effektive Benutzernummer eines Prozesses setzen (setreuid)             | XRU              | S/F    | -               | -       | M      | M        | M       | -    | M     | M    | -   | -      | -       | -       | -    | -   | -       | M       | -      | M    | -    | -       | -      | -   |
| Gruppennummer eines Prozesses setzen (setgid)                                    | XSG              | S/F    | -               | -       | M      | M        | M       | -    | M     | -    | M   | -      | -       | -       | -    | -   | -       | M       | -      | -    | -    | -       | -      | -   |
| Prozessgruppennummer einstellen (setpgrp)                                        | XSP              | S/F    | -               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | O       | O    | -   | -       | M       | -      | -    | M    | -       | -      | -   |
| Grenzwert für ein Betriebsmittel einstellen (setrlimit) <sup>1</sup>             | XSR <sup>1</sup> | S/F    | O               | O       | M      | M        | M       | -    | M     | -    | -   | O      | O       | -       | -    | -   | -       | M       | M      | -    | -    | -       | -      | -   |
| Benutzernummer eines Prozesses setzen (setuid)                                   | XSU              | S/F    | -               | -       | M      | M        | M       | -    | M     | -    | -   | -      | -       | -       | -    | -   | -       | M       | -      | -    | -    | -       | M      | -   |

<sup>1</sup> Die Felder curlim und curlim2, bzw. maxlim und maxlim2 schließen sich gegenseitig aus.  
 Wenn das Feld resourc den Wert CPU-TIME oder NO-OF-FILES hat, werden die Felder curlim und maxlim protokolliert;  
 ist resourc=FILE-SIZE, werden stattdessen die Felder curlim2 und maxlim2 protokolliert.

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| curlim   | *       | 0117 | Current limit<br>type: integer 0..2 <sup>31</sup> -1                      |
| curlim2  | *       | 0141 | Current limit (in multiple of 512)<br>type: integer 0..2 <sup>31</sup> -1 |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                |
|----------|---------|------|----------------------------------------------------------------------------------------------------------|
| curpid   | *       | 0100 | Current process id of the calling process<br>type: integer 0..2 <sup>31</sup> -1                         |
| currgid  | *       | 0102 | Current real POSIX group id of the calling process<br>type: integer 0..2 <sup>31</sup> -1                |
| curruid  | *       | 0101 | Current real POSIX user id of the calling process<br>type: integer 0..2 <sup>31</sup> -1                 |
| egid     | *       | 0116 | Effective POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                                          |
| errno    | *       | 0103 | POSIX error number<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                                |
| euid     | *       | 0113 | Effective POSIX user id<br>type: integer 0..2 <sup>31</sup> -1                                           |
| gid      | *       | 0114 | POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                                                    |
| maxlim   | *       | 0118 | Maximum limit<br>type: integer 0..2 <sup>31</sup> -1                                                     |
| maxlim2  | *       | 0142 | Maximum limit (in multiple of 512)<br>type: integer 0..2 <sup>31</sup> -1                                |
| pathnam  | *       | 0105 | Name of file resp. directory<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255) |
| pgid     | *       | 0110 | Process group id<br>type: integer 0..2 <sup>31</sup> -1                                                  |
| pid      | *       | 010F | Process id<br>type: integer 0..2 <sup>31</sup> -1                                                        |
| pidrecv  | *       | 010E | Process id of receiving process<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                   |
| resourc  | *       | 012C | Resource<br>keywords: CPU-TIME/FILE-SIZE/NO-OF-FILES                                                     |
| retval   | *       | 0104 | POSIX return value<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                                |
| rgid     | *       | 0115 | Real POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                                               |
| ruid     | *       | 0112 | Real POSIX user id<br>type: integer 0..2 <sup>31</sup> -1                                                |
| setpcmd  | *       | 012E | Suboperation for event XSP (set process group id)<br>keywords: SET-PGID/SET-SID/<br>SET-SID-AND-PGID     |

| <b>Feldname</b> | <b>A/Fil</b> | <b>exit</b> | <b>Bedeutung und Werte der Information:<br/>SDF-Datentyp oder Schlüsselwörter</b> |
|-----------------|--------------|-------------|-----------------------------------------------------------------------------------|
| signal          | *            | 012B        | Signal sent to a process<br>keywords: ABORT/KILL                                  |
| uid             | *            | 0111        | POSIX user id<br>type: integer 0.. $2^{31}-1$                                     |
| ulimcmd         | *            | 012F        | Suboperation for event XLM (set process limits)<br>keywords: SET-FILE-LIMIT       |



| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                           |
|----------|---------|------|-------------------------------------------------------------------------------------------------------------------------------------|
| dltsec   | *       | 0119 | Delta seconds for adjusting the system time<br>type: integer 0.. $2^{31}-1$                                                         |
| dltusec  | *       | 011A | Delta microseconds for adjusting the system time<br>type: integer 0.. $2^{31}-1$                                                    |
| errno    | *       | 0103 | POSIX error number<br>type: integer $-2^{31}..2^{31}-1$                                                                             |
| gid      | *       | 0114 | POSIX group id<br>type: integer 0.. $2^{31}-1$                                                                                      |
| homedir  | *       | 0108 | Home directory of a user<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)                                |
| nsems    | *       | 0123 | Total number of all semaphores<br>type: integer 0.. $2^{31}-1$                                                                      |
| obj-uid  | *       | 0011 | User identification as object<br>type: c-string 1..8                                                                                |
| procnam  | *       | 0019 | Processor name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                 |
| pwcmd    | *       | 0130 | Suboperation for event XPW (set user attributes)<br>keywords: FORK-WITH-USER-CHANGE/<br>MOD-POSIX-USER-ATTR/<br>POSIX-RLOGIN-ACCESS |
| retval   | *       | 0104 | POSIX return value<br>type: integer $-2^{31}..2^{31}-1$                                                                             |
| semact   | *       | 0133 | Action code for semaphore control operation<br>keywords: REMOVE-ID/SET-OPTIONS                                                      |
| semcmd   | *       | 0131 | Semaphore control operation<br>keywords: CONTROL/GET                                                                                |
| semid    | *       | 0121 | Id of the semaphore<br>type: integer 0.. $2^{31}-1$                                                                                 |
| semnum   | *       | 0122 | Number of a specific semaphore<br>type: integer 0.. $2^{31}-1$                                                                      |
| setsgid  | *       | 013C | Set the set-group-id bit<br>keywords: NO/YES                                                                                        |
| setsuid  | *       | 013B | Set the set-user-id bit<br>keywords: NO/YES                                                                                         |
| shell    | *       | 0109 | Shell of a user<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)                                         |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter           |
|----------|---------|------|-------------------------------------------------------------------------------------|
| shmact   | *       | 0134 | Action code for shared memory control operation<br>keywords: REMOVE-ID/SET-OPTIONS  |
| shmaddr  | *       | 011E | Address of the shared memory<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)   |
| shmcmd   | *       | 0132 | Shared memory control operation<br>keywords: ATTACH/CONTROL/DETACH/GET              |
| shmid    | *       | 0120 | Id of the shared memory<br>type: integer 0..2 <sup>31</sup> -1                      |
| shmrdo   | *       | 013E | Shared memory is read only<br>keywords: NO/YES                                      |
| shmsize  | *       | 011F | Size of the shared memory<br>type: integer 0..2 <sup>31</sup> -1                    |
| uid      | *       | 0111 | POSIX user id<br>type: integer 0..2 <sup>31</sup> -1                                |
| userkey  | *       | 0143 | User-selected numerical key<br>type : integer -2 <sup>31</sup> ..2 <sup>31</sup> -1 |

## Objekt PRIVILEGE

| Ereignis                              | evt | SAT-Information |         |       |         |
|---------------------------------------|-----|-----------------|---------|-------|---------|
|                                       |     | priv            | obj-uid | catid | privset |
| vergeben                              | PST | O               | M       | M     | O       |
| entziehen                             | PRT | O               | M       | M     | O       |
| Sammelprivileg erzeugen               | PSC | O               | -       | M     | M       |
| Sammelprivileg löschen                | PSD | -               | -       | M     | M       |
| Privileg zu Sammelprivileg hinzufügen | PSA | M               | -       | M     | M       |
| Privileg aus Sammelprivileg entfernen | PSR | M               | -       | M     | M       |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                             |
|----------|-------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catid    | *     | 0022 | Catalog identifier<br>type: c-string 1..4                                                                                                                                             |
| obj-uid  | *     | 0011 | User identifier as object<br>type: c-string 1..8                                                                                                                                      |
| priv     | *     | 002D | Processed privilege identification<br>keywords: siehe „Tabelle der Privilegien“ im Handbuch „ <a href="#">SECOS - Security Control System - Zugangs- und Zugriffskontrolle</a> “ [1]. |
| privset  | *     | 00A3 | privilege set name<br>type: c-string 1..8                                                                                                                                             |

## Objekt PROGRAM

| Ereignis                   | evt | res | SAT-Information |                |                |         |         |         |         |         |         |         |        |         |       |   |
|----------------------------|-----|-----|-----------------|----------------|----------------|---------|---------|---------|---------|---------|---------|---------|--------|---------|-------|---|
|                            |     |     | cxtname         | filename       | eltname        | eltvers | elttype | intname | intvers | intdate | loaduni | memclas | ldvers | mempool | scope |   |
| Phase laden aus PAM-Datei  | XLD | S   | M               | M <sup>1</sup> | -              | -       | -       | M       | M       | M       | M       | M       | M      | -       | O     | O |
| Phase laden aus Bibliothek | XLD | S   | M               | M <sup>2</sup> | M              | M       | M       | M       | M       | M       | M       | M       | M      | M       | O     | O |
| Phase laden                | XLD | F   | O               | M              | O              | O       | O       | O       | O       | O       | O       | O       | M      | O       | O     | O |
| LLM laden aus Bibliothek   | XLD | S   | M               | M <sup>2</sup> | M              | M       | M       | M       | M       | M       | M       | M       | M      | M       | O     | O |
| OM laden aus EAM           | XLD | S   | M               | M <sup>3</sup> | M <sup>4</sup> | -       | M       | M       | -       | -       | M       | M       | -      | O       | O     | O |
| OM laden aus Bibliothek    | XLD | S   | M               | M <sup>2</sup> | M              | M       | M       | M       | M       | -       | -       | M       | M      | M       | O     | O |
| Modul laden                | XLD | F   | O               | M <sup>2</sup> | O              | O       | O       | O       | O       | O       | O       | O       | M      | -       | O     | O |
| entladen                   | XUL | S   | M               | -              | -              | -       | -       | O       | -       | -       | O       | -       | O      | O       | O     | O |
|                            |     | F   | M               | -              | -              | -       | -       | O       | -       | -       | O       | -       | O      | O       | O     | O |

LLM = link and load module

OM = object module

<sup>1</sup> Name der Phase

<sup>2</sup> Name der Bibliotheksdatei

<sup>3</sup> Das Feld enthält einen Stern (\*)

<sup>4</sup> Das Feld enthält Leerzeichen

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| cxtname  | *     | 000F | Context name<br>type: c-string 1..32                                      |
| eltname  | *     | 0008 | Element name<br>type: c-string 1..64                                      |
| elttype  | *     | 000A | Element type<br>type: c-string 1..8                                       |
| eltvers  | *     | 0009 | Element version<br>type: c-string 1..24                                   |
| filename | *     | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |
| intdate  | *     | 000D | Internal date<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)        |
| intname  | *     | 000B | Internal name<br>type: c-string 1..41                                     |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter         |
|----------|---------|------|-----------------------------------------------------------------------------------|
| intvers  | *       | 000C | Internal version<br>type: c-string 1..24                                          |
| ldvers   | *       | 0099 | Load unit version<br>type: c-string 1..24                                         |
| loaduni  | *       | 000E | Load unit name<br>type: c-string 1..32                                            |
| memclas  | *       | 0020 | memory class of the memory pool<br>keywords: CLASS3/CLASS4/CLASS5/CLASS6          |
| mempool  | *       | 001C | memory pool name<br>type: c-string 1..54                                          |
| scope    | *       | 001D | Memory pool scope<br>keywords: LOCAL/GROUP/GLOBAL/USER-GROUP/<br>UNDEFINED/SYSTEM |

Objekt SAT

| Ereignis                 | evt | res | SAT-Information |         |       |        |         |        |          |         |         |         |         |         |         |         |        |        |      |        |        |         |        |        |       |        |         |         |         |      |
|--------------------------|-----|-----|-----------------|---------|-------|--------|---------|--------|----------|---------|---------|---------|---------|---------|---------|---------|--------|--------|------|--------|--------|---------|--------|--------|-------|--------|---------|---------|---------|------|
|                          |     |     | blksize         | confnam | cpuid | device | dodvers | evtaud | filename | logquan | newfile | obj-evt | obj-uid | periodd | periodh | priallo | prexit | reason | rule | savpar | savval | secallo | suppar | supval | sysid | sysnam | sysvers | uauddef | useraud | vsn1 |
| Kommando                 | ZHO | S   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       | -    |
| HOLD-SAT-LOGGING         |     | F   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| Kommando RESUME-         | ZRE | S   | -               | -       | -     | -      | -       | -      | -        | M       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| SAT-LOGGING              |     | F   | -               | -       | -     | -      | -       | -      | O        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| Kommando MODIFY-         | ZPS | S   | -               | -       | -     | -      | -       | O      | -        | O       | -       | O       | O       | -       | -       | -       | O      | -      | O    | -      | -      | -       | -      | -      | -     | -      | O       | O       | -       |      |
| SAT-PRESELECTION         |     | F   | -               | -       | -     | -      | -       | O      | -        | O       | -       | O       | O       | -       | -       | -       | O      | -      | O    | -      | -      | -       | -      | -      | -     | -      | O       | O       | -       |      |
| Kommando MODIFY-SAT-     | ZMS | S   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | O      | O      | -     | -      | -       | -       | -       |      |
| SUPPORT-PARAMETERS       |     | F   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | O      | O      | -     | -      | -       | -       | -       |      |
| Kommando                 | ZCH | S   | M               | -       | -     | O      | -       | M      | -        | -       | -       | -       | O       | O       | M       | -       | -      | -      | -    | -      | M      | -       | -      | -      | -     | -      | -       | O       | -       |      |
| CHANGE-SAT-FILE          |     | F   | O               | -       | -     | O      | -       | O      | -        | -       | -       | -       | O       | O       | O       | -       | -      | -      | -    | -      | -      | O       | -      | -      | -     | -      | -       | O       | -       |      |
| Kommando SAVE-           | ZSP | S   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | O      | O      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| SAT-PARAMETERS           |     | F   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | O    | O      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| HEADER-Satz              | ZBG | -   | -               | M       | M     | -      | M       | -      | O        | -       | M       | -       | -       | -       | -       | -       | M      | -      | -    | -      | -      | -       | -      | M      | M     | M      | -       | -       | -       |      |
| TRAILER-Satz             | ZND | -   | -               | -       | -     | -      | M       | -      | O        | -       | -       | -       | -       | -       | -       | -       | M      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| SAT Event Preselection   | ZEP | S   | -               | -       | -     | -      | -       | M      | -        | -       | -       | M       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |
| when selection file open |     | F   | -               | -       | -     | -      | -       | -      | -        | -       | -       | -       | -       | -       | -       | -       | -      | -      | -    | -      | -      | -       | -      | -      | -     | -      | -       | -       | -       |      |

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| blksize  | *      | 00CD | block size<br>type: integer, sensible values 1..32767                     |
| confnam  |        | 008B | configuration name<br>type: c-string 1..21                                |
| cpuid    |        | 008D | cpu identification<br>type: x-string 2..128                               |
| device   | *      | 003C | Device name<br>type: c-string 1..8                                        |
| dodvers  |        | 009A | dod version<br>type: c-string 1..7                                        |
| evtaud   | *      | 00CE | event auditability<br>keywords: SUCCESS/FAILURE/ALL/NONE                  |
| filename | *      | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                  |
|----------|---------|------|----------------------------------------------------------------------------------------------------------------------------|
| logquan  | *       | 00F9 | sign for logging quantity<br>type: c-string 1..8                                                                           |
| newfile  | *       | 0007 | New file name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                                             |
| obj-evt  | *       | 00C9 | event as object<br>type: c-string 1..3                                                                                     |
| obj-uid  | *       | 0011 | User identifier as object<br>type: c-string 1..8                                                                           |
| periodd  | *       | 00EA | number of days for action repetition<br>type: integer 0..255                                                               |
| periodh  | *       | 00EB | number of hours for action repetition<br>type: integer 0..255                                                              |
| prexit   | *       | 00D0 | Exit routine activated<br>keywords: YES/NO                                                                                 |
| priallo  | *       | 00CB | primary allocation<br>type: integer $-2^{31}..2^{31}-1$                                                                    |
| reason   | *       | 008C | reason<br>keywords: RESUME-SAT-LOGGING/ CHANGE-SAT-FILE/DMS-ERROR/<br>HOLD-SAT-LOGGING/SHUTDOWN/PERIODIC-SWITCHING/STARTUP |
| rule     | *       | 00CA | rule<br>keywords: FILES-BY-EVENT/<br>INDEPENDENT/UNCHANGED                                                                 |
| savpar   | *       | 00D1 | saved parameters<br>keywords: ALARM/FILTER/LOGGING-FILE-ATTRIBUTES/<br>PRESELECTION/SAT-SUPPORT                            |
| savval   | *       | 00D2 | saved value<br>keywords: CURRENT/STANDARD                                                                                  |
| secallo  | *       | 00CC | secondary allocation<br>type: integer $-2^{31}..2^{31}-1$                                                                  |
| suppar   | *       | 013F | name of SAT support parameter<br>keywords: POSIX-EVENTS                                                                    |
| supval   | *       | 0140 | value of SAT support parameter<br>keywords: DISABLED / ENABLED                                                             |
| sysid    |         | 0088 | system-id<br>type: c-string 1..3                                                                                           |
| sysnam   |         | 0089 | system-name<br>type: c-string 1..8                                                                                         |

| <b>Feldname</b> | <b>A/I/Fil</b> | <b>exit</b> | <b>Bedeutung und Werte der Information:<br/>SDF-Datentyp oder Schlüsselwörter</b> |
|-----------------|----------------|-------------|-----------------------------------------------------------------------------------|
| sysvers         |                | 008A        | system version<br>type: c-string 1..4                                             |
| useraud         | *              | 00CF        | user auditability<br>keywords: YES/NO                                             |
| vsn1            | *              | 0039        | volume serial number<br>type: c-string 1..6                                       |

## Objekt SAT-ALARM

| Ereignis                                                          | evt              | res | SAT-Information |        |         |        |         |        |          |         |         |
|-------------------------------------------------------------------|------------------|-----|-----------------|--------|---------|--------|---------|--------|----------|---------|---------|
|                                                                   |                  |     | almact          | almlim | almname | almrep | almssel | evtaud | obj-flid | obj-evt | obj-uid |
| Kommando ADD-SAT-ALARM-CONDITIONS                                 | ZCA              | S   | -               | -      | M       | -      | -       | -      | -        | -       | -       |
|                                                                   |                  | F   | -               | -      | O       | -      | -       | -      | -        | -       | -       |
| Kommando REMOVE-SAT-ALARM-CONDITIONS                              | ZDA              | S   | -               | -      | M       | -      | -       | -      | -        | -       | -       |
|                                                                   |                  | F   | -               | -      | O       | -      | -       | -      | -        | -       | -       |
| Kommando MODIFY-SAT-ALARM-CONDITIONS (Alarmauslöser) <sup>1</sup> | ZMA              | S   | O               | O      | M       | O      | O       | O      | O        | O       | O       |
|                                                                   |                  | F   | O               | O      | O       | O      | O       | O      | O        | O       | O       |
|                                                                   | ZAL <sup>1</sup> | -   | M               | -      | M       | -      | -       | M      | -        | M       | -       |

<sup>1</sup> Zusätzlich zu den angegebenen Feldern werden alle Felder des Ereignisses protokolliert, durch das der Alarm ausgelöst wurde.

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| almact   | *      | 00D6 | alarm action<br>keywords: OPERATOR-MESSAGE/OPERATOR-PAUSE                 |
| almlim   | *      | 00D4 | alarm time limit (in seconds)<br>type: integer -1..2 <sup>31</sup> -1     |
| almname  | *      | 00D3 | alarm name<br>type: c-string 1..8                                         |
| almrep   | *      | 00D5 | alarm repeat<br>type: integer 0..255                                      |
| almssel  | *      | 00D7 | alarm selection<br>keywords: ON/OFF                                       |
| evtaud   | *      | 00CE | event auditability<br>keywords: SUCCESS/FAILURE/ALL/NONE                  |
| obj-evt  | *      | 00C9 | event as object<br>type: c-string 1..3 (ALARM/FILTER: c-string 3..3)      |
| obj-flid | *      | 00D8 | object field<br>type: c-string 1..7                                       |
| obj-uid  | *      | 0011 | User identifier as object<br>type: c-string 1..8                          |

## Objekt SAT-FILTER

| Ereignis                              | evt | res | SAT-Information |         |        |
|---------------------------------------|-----|-----|-----------------|---------|--------|
|                                       |     |     | ffrac           | ftrname | ftrsel |
| Kommando ADD-SAT-FILTER-CONDITIONS    | ZCF |     | M               | M       | -      |
| Kommando REMOVE-SAT-FILTER-CONDITIONS | ZDF |     | -               | M       | -      |
| Kommando MODIFY-SAT-FILTER-CONDITIONS | ZMF |     | M               | M       | O      |

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| ffrac    | *      | 00FA | Filter Action Logging on/off<br>keywords: NO-RECORDING/RECORDING          |
| ftrname  | *      | 00FB | Filter Name<br>Type: c-string 1..8                                        |
| ftrsel   | *      | 00FC | Filter selection<br>keywords: OFF/ON                                      |

## Objekt SESAM

| Ereignis                                            | evt | res | SAT-Information |         |         |        |        |         |         |        |         |         |         |         |        |         |
|-----------------------------------------------------|-----|-----|-----------------|---------|---------|--------|--------|---------|---------|--------|---------|---------|---------|---------|--------|---------|
|                                                     |     |     | applnam         | appluid | dbhconf | dbhnam | dbname | dbtable | hostnam | schema | sessubc | sestext | stmtctf | stmtcts | utmsct | utmuser |
| DBH-Session administrieren                          | SEA | S   | M               | O       | M       | M      | -      | -       | M       | -      | M       | M       | -       | -       | M      | M       |
|                                                     |     | F   | M               | O       | M       | M      | -      | -       | M       | -      | M       | M       | -       | -       | M      | M       |
| Zugriffsrechte und Benutzerzugänge ändern           | SEP | S   | M               | O       | M       | M      | M      | -       | M       | -      | M       | O       | -       | -       | M      | M       |
|                                                     |     | F   | M               | O       | M       | M      | M      | -       | M       | -      | M       | O       | -       | -       | M      | M       |
| DDL-, SSL-, Utility-Anweisung                       | SES | S   | M               | O       | M       | M      | M      | O       | M       | O      | M       | O       | -       | -       | M      | M       |
|                                                     |     | F   | M               | O       | M       | M      | M      | O       | M       | O      | M       | O       | -       | -       | M      | M       |
| SESAM-Task (DBH- oder Service-Task) starten/beenden | SET | S   | -               | -       | M       | M      | -      | -       | -       | -      | M       | M       | -       | -       | -      | -       |
|                                                     |     | F   | -               | -       | M       | M      | -      | -       | -       | -      | M       | M       | -       | -       | -      | -       |
| Vorgang beenden                                     | SEU | S   | M               | O       | M       | M      | -      | -       | M       | -      | M       | -       | M       | M       | M      | M       |
|                                                     |     | F   | M               | O       | M       | M      | -      | -       | M       | -      | M       | -       | M       | M       | M      | M       |

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                |
|----------|---------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| applnam  | *       | 0025 | Application name<br>type: c-string 1..8<br>In case of a TIAM program the field contains the string 'TSN=<tsn>' where <tsn> stands for the tsn of the application program |
| appluid  | *       | 0162 | Application user id<br>type: c-string 1..8                                                                                                                               |
| dbhconf  | *       | 0160 | DBH configuration identifier<br>type: c-string 1..1                                                                                                                      |
| dbhnam   | *       | 015F | DBH name identifier<br>type: c-string 1..1                                                                                                                               |
| dbname   | *       | 0165 | Logical database name<br>type: c-string 1..18                                                                                                                            |
| dbtable  | *       | 0167 | Table name in the catalog<br>type: c-string 1..31                                                                                                                        |
| hostnam  | *       | 0029 | Name of the host<br>type: c-string 1..8                                                                                                                                  |
| schema   | *       | 0166 | Schema name in the catalog<br>type: c-string 1..31                                                                                                                       |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sessubc  | *       | 015E | Subcode for the SESAM events<br>type: c-string 1..4<br>Abhängig vom jeweiligen Event sind folgende Subcodes auswertbar:<br><b>Event SET</b><br>– STRT: Start of a SESAM-DBH-Task<br>– END: End of a SESAM-DBH-Task<br><b>Event SEU</b><br>– END: End of a session<br><b>Event SEA</b><br>– ADM Administration stmt<br><b>Event SEP</b><br>– USR: Add/remove/modify users<br>– PRI: Grant/revoke rights<br><b>Event SES</b><br>– DDL: DDL stmt<br>– SSL: SSL stmt<br>– UTI: Utility stmt |
| sestext  | *       | 0168 | Additional information for the SESAM events<br>type: c-string 1..64                                                                                                                                                                                                                                                                                                                                                                                                                     |
| stmtctf  | *       | 0164 | Number of unsuccessful statements in the session<br>type: integer 0..2 <sup>31</sup> -1<br>A statement is unsuccessful if it is not confirmed with "successful completion", "no data" or "rollback".                                                                                                                                                                                                                                                                                    |
| stmtcts  | *       | 0163 | Number of successful statements in the session<br>type: integer 0..2 <sup>31</sup> -1<br>A statement is successful if it is confirmed with "successful completion", "no data" or "rollback".                                                                                                                                                                                                                                                                                            |
| utmsct   | *       | 0161 | UTM session counter<br>type: x-string 2..16 (ALARM/FILTER: x-string 16..16)                                                                                                                                                                                                                                                                                                                                                                                                             |
| utmuser  | *       | 0048 | User id in UTM application frame<br>type: c-string 1..8                                                                                                                                                                                                                                                                                                                                                                                                                                 |

*Zusatzinformation zu einzelnen Datenfeldern*

*(siehe auch Handbuch „SESAM/SQL-Server – Datenbankbetrieb“ [33])*

- Mit den Feldern dbhnam und dbhconf können die SAT-Protokollsätze aller Tasks eines Data Base Handlers identifiziert werden.
- Mit den Feldern hostnam, applnam, utmuser und utmsct kann ein bestimmter Vorgang identifiziert werden.

- Bei der Protokollierung eines Administrationskommandos über /SEND-MSG sind einige Felder nicht oder nur auf bestimmte Weise versorgt:

| Feldname | Inhalt         |
|----------|----------------|
| hostnam  | 'SESAM'        |
| applnam  | 'SEND'         |
| utmuser  | 'MESSAGE'      |
| appluid  | nicht versorgt |

## Objekt SMS

| Ereignis                                      | evt | SAT-Information |         |         |        |       |
|-----------------------------------------------|-----|-----------------|---------|---------|--------|-------|
|                                               |     | catid           | newvset | storcla | volset | vslst |
| Speicherklasse einrichten                     | SCC | M               | -       | M       | -      | -     |
| Eigenschaften der Speicherklasse ändern       | SCM | M               | -       | M       | -      | -     |
| Speicherklasse löschen                        | SCD | M               | -       | M       | -      | -     |
| Speicherklasse an volume-set-list koppeln     | SCB | M               | -       | M       | -      | M     |
| PVSREN: alle Speicherklassen löschen          | SCP | M               | -       | M       | -      | -     |
| Speicherklasse von volume-set-list entkoppeln | SCU | M               | -       | M       | -      | M     |
| Kommando CHANGE-STORAGE-CLASS-CATALOG         | SCX | M               | -       | -       | -      | -     |
| Volume-set-list einrichten                    | VLC | M               | -       | -       | -      | M     |
| Volume-set-list ändern                        | VLM | M               | -       | -       | -      | M     |
| Volume-set-list löschen                       | VLD | M               | -       | -       | -      | M     |
| Volume-set in volume-set-list eintragen       | VLA | M               | -       | -       | M      | M     |
| Volume-set aus volume-set-list entfernen      | VLR | M               | -       | -       | M      | M     |
| Kommando CHANGE-VOLUME-SET-LIST-CATALOG       | VLX | M               | -       | -       | -      | -     |
| PVSREN: volume-set umbenennen                 | VP1 | M               | M       | -       | M      | M     |
| PVSREN: alle volume-sets umbenennen           | VP2 | M               | -       | -       | -      | M     |
| PVSREN: alle volume-set-lists löschen         | VP3 | M               | -       | -       | -      | M     |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| catid    | *       | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| newvset  | *       | 00D9 | New volume set name<br>type: c-string 1..4                                |
| storcla  | *       | 00ED | storage class<br>type: c-string 1..8                                      |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| volset   | *     | 00EF | volume set<br>type: c-string 1..4                                         |
| vslist   | *     | 00EE | volume set list<br>type: c-string 1..8                                    |

## Objekt SPOOL DEVICE

| Ereignis             | evt | SAT-Information |       |         |         |
|----------------------|-----|-----------------|-------|---------|---------|
|                      |     | device          | admin | station | procnam |
| RSO-Gerät definieren | SDA | M               | O     | O       | O       |
| Eigenschaften ändern | SDM | M               | O     | O       | O       |
| Eintrag löschen      | SDR | M               | -     | -       | -       |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| admin    | *     | 002B | (Group)administrator identification<br>type: c-string 1..8 (user-id)      |
| device   | *     | 003C | Device name<br>type: c-string 1..8                                        |
| procnam  | *     | 0019 | Processor name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)       |
| station  | *     | 0018 | Terminal name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)        |

## Objekt SPOOL JOBS

| Ereignis         | evt | res | SAT-Information |        |       |         |         |         |       |                       |                      |        |         |         |         |         |         |        |         |
|------------------|-----|-----|-----------------|--------|-------|---------|---------|---------|-------|-----------------------|----------------------|--------|---------|---------|---------|---------|---------|--------|---------|
|                  |     |     | destsup         | device | dmsrc | eltname | elttype | eltvers | erase | filename <sup>1</sup> | fnpatrn <sup>1</sup> | jobcmd | jobcopy | joberrt | joborig | jobpage | jobterm | plamrc | tsn-inf |
| Druck anfordern  | JPR | S   | -               | -      | -     | O       | O       | O       | M     | M                     | -                    | -      | -       | -       | -       | -       | -       | -      | M       |
|                  |     | F   | -               | -      | O     | O       | O       | M       | O     | O                     | -                    | -      | -       | -       | -       | -       | -       | -      | -       |
| Job löschen      | JPC | S   | -               | -      | -     | O       | -       | -       | -     | -                     | -                    | -      | -       | -       | -       | -       | -       | -      | M       |
|                  |     | F   | -               | -      | -     | -       | -       | -       | -     | -                     | -                    | -      | -       | -       | -       | -       | -       | -      | -       |
| Druck beendet    | JPE | S   | M               | M      | O     | O       | O       | O       | O     | M                     | -                    | M      | O       | M       | M       | O       | M       | -      | M       |
|                  |     | F   | M               | M      | O     | O       | O       | O       | O     | M                     | -                    | M      | O       | M       | M       | O       | M       | O      | M       |
| Job unterbrechen | JPI | S   | M               | M      | O     | O       | O       | O       | O     | M                     | -                    | M      | O       | M       | M       | O       | M       | -      | M       |
|                  |     | F   | M               | M      | O     | O       | O       | O       | O     | M                     | -                    | M      | O       | M       | M       | O       | M       | O      | M       |

<sup>1</sup> schließen sich gegenseitig aus

| Feldname | A/I/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|---------|------|---------------------------------------------------------------------------|
| destsup  | *       | 00A4 | destination (output support)<br>keywords: LOCAL/REMOTE/TAPE               |
| device   | *       | 003C | Device name<br>type: c-string 1..8                                        |
| dmsrc    | *       | 0004 | DMS return code<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)      |
| eltname  | *       | 0008 | Element name<br>type: c-string 1..64                                      |
| elttype  | *       | 000A | Element type<br>type: c-string 1..8                                       |
| eltvers  | *       | 0009 | Element version<br>type: c-string 1..24                                   |
| erase    | *       | 0041 | File deletion status<br>keywords: YES/NO                                  |
| filename | *       | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |
| fnpatrn  | *       | 0063 | filename pattern<br>type: c-string 1..80                                  |
| jobcmd   | *       | 00A7 | job command origin<br>keywords: PRINT                                     |
| jobcopy  | *       | 00A8 | copies number<br>type: integer 0..255                                     |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                            |
|----------|---------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| joberrt  | *       | 00AA | detected errors during spoolout<br>keywords: DEVICERR/DMS/<br>NONE/PLAM/SYSTEM/USER                                                                                                                                                                                  |
| joborig  | *       | 00A6 | job origin<br>keywords: NORMAL/RTCOPY/RTDIRECT                                                                                                                                                                                                                       |
| jobpage  | *       | 00A9 | printed pages number<br>type: integer: $0..2^{31}-1$                                                                                                                                                                                                                 |
| jobterm  | *       | 00A5 | Termination or interruption type<br>keywords: ABORT/CANCEL/KEEP<br>NORMAL/RESPOOL/SUSPEND                                                                                                                                                                            |
| plamrc   | *       | 0046 | PLAM return code<br>type: c-string 1..13 (ALARM/FILTER: x-string 16..16).<br>Format: zzzz/xxxxxxx<br>zzzz = Primärkode (Dezimal)<br>xxxxxxx= Sekundärkode (Sedezimal)<br>Mit /HELP PLAzxxx kann Information über den entsprechenden Return-<br>code abgerufen werden |
| tsn-inf  | *       | 0010 | TSN object<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)                                                                                                                                                                                                      |

## Objekt SUBSYSTEM

| Ereignis                                            | evt | res | SAT-Information |         |         |        |         |         |         |         |         |         |       |       |   |
|-----------------------------------------------------|-----|-----|-----------------|---------|---------|--------|---------|---------|---------|---------|---------|---------|-------|-------|---|
|                                                     |     |     | cat             | cxtname | libname | replib | subsnam | subsver | synfile | inffile | msgfile | obj-uid | sscmd | sshld |   |
| aktivieren                                          | SCR | S/F | -               | M       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
| deaktivieren                                        | SDL | S   | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
|                                                     |     | F   | -               | -       | -       | -      | -       | -       | -       | -       | -       | -       | -     | -     | - |
| anhalten                                            | SHD | S/F | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
| fortsetzen                                          | SRS | S/F | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
| Konnektierung mit nicht privilegiertem Subsystem    | SCN | S   | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
| Diskonnektierung von nicht privilegiertem Subsystem | SDS | S   | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
|                                                     |     | F   | -               | -       | -       | -      | -       | -       | -       | -       | -       | -       | -     | -     | - |
| Katalogverwaltung                                   | SCT | S/F | M               | -       | -       | -      | -       | -       | -       | -       | -       | -       | -     | -     | - |
| Subsystem-Teil laden                                | SLP | S/F | -               | O       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |
| Subsystem-Datei wechseln                            | SFC | S/F | -               | O       | O       | O      | M       | M       | O       | O       | O       | O       | O     | O     | O |
| Subsystem entfernen                                 | SRM | S/F | -               | -       | -       | -      | M       | M       | -       | -       | -       | -       | -     | -     | - |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter  |
|----------|-------|------|----------------------------------------------------------------------------|
| cat      | *     | 0032 | New catalog name<br>type: c-string 1..54 (ALARM/FILTER: filename)          |
| cxtname  | *     | 000F | Context name<br>type: c-string 1..32                                       |
| inffile  | *     | 00E5 | information file<br>type: c-string 1..54 (ALARM/FILTER: filename)          |
| libname  | *     | 00A0 | object module library<br>type: c-string 1..54 (ALARM/FILTER: filename)     |
| msgfile  | *     | 00E4 | message file<br>type: c-string 1..54 (ALARM/FILTER: filename)              |
| obj-uid  | *     | 0011 | user identifier as object<br>type: c-string 1..8                           |
| replib   | *     | 00A1 | rep file name<br>type: c-string 1..54 (ALARM/FILTER: filename)             |
| sscmd    | *     | 00E7 | DSSM commands permission<br>Keyword: ALLOWED/BY-ADMINISTRATOR/FORBIDDEN    |
| sshld    | *     | 00E6 | Indicates if subsystem can be deleted / held<br>Keyword: ALLOWED/FORBIDDEN |

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| subsnam  | *      | 0030 | name of the subsystem<br>type: c-string 1..8                              |
| subsver  | *      | 0031 | version of the subsystem<br>type: c-string 1..7                           |
| synfile  | *      | 00A2 | syntax file name<br>type: c-string 1..54 (ALARM/FILTER: filename)         |

## Objekt SYNTAX FILE

| Ereignis                            | evt | res | SAT-Information |         |        |
|-------------------------------------|-----|-----|-----------------|---------|--------|
|                                     |     |     | filename        | syntype | sdfcmd |
| aktivieren                          | YAC | S/F | M               | M       | -      |
| modifizieren                        | YMD | S/F | M               | M       | -      |
| Hierarchie eröffnen (Makro OPNCALL) | YON | S/F | M               | M       | -      |
| für Subsystem aktivieren            | YAD | S/F | M               | M       | -      |
| überprüfen                          | YCK | S   | -               | -       | -      |
|                                     |     | F   | M               | M       | M      |

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| filename | *      | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |
| sdfcmd   | *      | 00AC | SDF command name<br>type: c-string 1..30                                  |
| syntype  | *      | 002E | Syntax file type<br>keywords: SYSTEM/GROUP/SUBSYSTEM/USER                 |

## Objekt TAPE encryption

| Ereignis                                    | evt | SAT-Information |        |         |         |        |       |         |        |         |         |         |         |         |      |
|---------------------------------------------|-----|-----------------|--------|---------|---------|--------|-------|---------|--------|---------|---------|---------|---------|---------|------|
|                                             |     | acctokb         | dpthin | dpthost | hostnam | keybox | keyid | srchost | srctsn | srcuser | tgthost | tgtkbox | trfkbox | volkind | vsn1 |
| <b>TAPE encryption</b>                      |     |                 |        |         |         |        |       |         |        |         |         |         |         |         |      |
| Anweisung<br>CREATE-ENCRYPTION-KEY          | TKC | -               | -      | -       | M       | M      | O     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung<br>ADD-ENCRYPTION-KEY             | TKA | -               | -      | -       | M       | M      | M     | -       | -      | -       | -       | -       | -       | O       | -    |
| Anweisung<br>COPY-ENCRYPTION-KEYS           | TKP | -               | -      | -       | M       | M      | M     | -       | -      | -       | M       | M       | -       | -       | -    |
| Anweisung<br>REMOVE-ENCRYPTION-KEY          | TKR | -               | -      | -       | M       | M      | M     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung<br>SHOW-ENCRYPTION-KEYS           | TKS | -               | -      | -       | M       | M      | M     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung SET-WRITE-<br>ENCRYPTION-KEY      | TWK | -               | -      | -       | M       | M      | M     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung<br>DELETE-KEY-BOX                 | TBD | -               | -      | -       | M       | M      | -     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung<br>EXPORT-KEY-BOX                 | TBE | -               | M      | O       | M       | M      | -     | -       | -      | -       | -       | M       | -       | -       | -    |
| Anweisung<br>IMPORT-KEY-BOX                 | TBI | -               | -      | M       | -       | -      | -     | -       | -      | M       | M       | M       | -       | -       | -    |
| Anweisung<br>REPAIR-KEY-BOX                 | TBR | -               | -      | -       | M       | M      | -     | -       | -      | -       | -       | -       | -       | -       | -    |
| Anweisung MODIFY-VOLUME-<br>ENCRYPTION-ATTR | TVM | -               | -      | -       | -       | -      | M     | -       | -      | -       | -       | -       | -       | O       | M    |
| Anweisung SHOW-VOLUME-<br>ENCRYPTION-ATTR   | TVS | -               | -      | -       | -       | -      | -     | -       | -      | -       | -       | -       | -       | -       | M    |
| Zugriff auf key box                         | TBA | M               | -      | -       | M       | M      | -     | M       | M      | M       | -       | -       | -       | -       | -    |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter        |
|----------|-------|------|----------------------------------------------------------------------------------|
| acctokb  | *     | 0070 | access mode to the key box<br>keywords: OPEN-READ / OPEN-WRITE / DELETE / REPAIR |
| dpthin   | *     | 006B | Information about the depot host<br>keywords:<br>IMPORT-PROCESS-HOST/OWN         |
| dpthost  | *     | 006D | name of the host where the transfer key box is deposited<br>type: c-string 1..8  |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                      |
|----------|---------|------|------------------------------------------------------------------------------------------------------------------------------------------------|
| hostnam  | *       | 0029 | Name of the host<br>type: c-string 1..8                                                                                                        |
| keybox   | *       | 0066 | Key box name<br>type: c-string 1..54                                                                                                           |
| keyid    | *       | 0067 | Identification string for the encryption key<br>type: c-string 1..18<br>(ALARM/FILTER: c-string 18..18)                                        |
| srchost  | *       | 006F | Host from which the key box is accessed<br>type: c-string 1..8                                                                                 |
| srctsn   | *       | 0071 | TSN of the accessing subject<br>type: c-string 1..4                                                                                            |
| srcuser  | *       | 0072 | Userid of the accessing subject<br>type: c-string 1..8                                                                                         |
| tgthost  | *       | 0068 | Name of target host<br>type: c-string 1..8                                                                                                     |
| tgtkbox  | *       | 0069 | Name of target key box<br>type: c-string 1..54                                                                                                 |
| trfkbox  | *       | 006A | Name of transfer key box<br>type: c-string 1..54                                                                                               |
| volkind  | *       | 006E | Kind of volumes for which the key can be used resp. for which the encryption attributes are modified<br>keywords:<br>FROM-FOREIGN-MAREN-DOMAIN |
| vsn1     | *       | 0039 | volume serial number<br>type: c-string 1..6                                                                                                    |

## Objekt TERMINAL SET

| Ereignis | evt | SAT-Information |          |          |          |        |        |        |         |         |  |
|----------|-----|-----------------|----------|----------|----------|--------|--------|--------|---------|---------|--|
|          |     | catid           | nwtstnam | nwtstown | nwtstscp | partsb | partsm | tsname | tsowner | tsscope |  |
| erzeugen | TSB | M               | -        | -        | -        | E      | -      | M      | M       | M       |  |
| kopieren | TSC | M               | M        | M        | M        | -      | -      | M      | M       | M       |  |
| löschen  | TSD | M               | -        | -        | -        | -      | -      | M      | M       | M       |  |
| ändern   | TSM | M               | -        | -        | -        | -      | E      | M      | M       | M       |  |

| Feldname | AI/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|--------|------|---------------------------------------------------------------------------|
| catid    | *      | 0022 | Catalog identifier<br>type: c-string 1..4                                 |
| nwtstnam | *      | 00C6 | Name of new terminal set<br>type: c-string 1..8                           |
| nwtstown | *      | 00C8 | Owner of new terminal set<br>type: c-string 1..8                          |
| nwtstscp | *      | 00C7 | Scope of new terminal set<br>keyword: GROUP / SYSTEM / USER               |
| partsb   | +      | 0217 | Parameter list for build terminal set<br>type: x-string 2..200            |
| partsm   | +      | 0218 | Parameter list for modify terminal set<br>type: x-string 2..6800          |
| tsname   | *      | 00C3 | Terminal set name<br>type: c-string 1..8                                  |
| tsowner  | *      | 00C5 | Terminal set owner<br>type: c-string 1..8                                 |
| tsscope  | *      | 00C4 | Terminal set scope<br>keyword: GROUP / SYSTEM / USER                      |

## Objekt USERID

| Ereignis                                   | evt | SAT-Information |         |         |         |        |        |        |         |         |      |         |         |         |        |       |
|--------------------------------------------|-----|-----------------|---------|---------|---------|--------|--------|--------|---------|---------|------|---------|---------|---------|--------|-------|
|                                            |     | catid           | chkmode | groupnr | obj-uid | oprole | parlog | parpos | princll | procnam | rejr | routcod | station | uparmup | uparus | usern |
| hinzufügen                                 | UAD | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | E      | -     |
| Attribute modifizieren                     | UMD | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | E      | -     |
| entfernen                                  | URM | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| sperrern                                   | ULK | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| entsperren                                 | UUL | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| prüfen                                     | UCK | -               | M       | -       | M       | -      | -      | -      | O       | O       | O    | -       | O       | -       | -      | -     |
| Schutzattribute festlegen                  | USL | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| Schutzattribute modifizieren               | UML | M               | -       | -       | M       | -      | E      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| Kennwortschutz modifizieren                | UMP | M               | -       | -       | M       | -      | E      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| Kommando REQUEST-<br>OPERATOR-ROLE         | UOP | -               | -       | -       | M       | O      | -      | -      | -       | -       | O    | O       | -       | -       | -      | -     |
| Kommando MODIFY-<br>POSIX-USER-ATTRIBUTES  | UPA | M               | -       | O       | -       | -      | -      | E      | -       | -       | -    | -       | -       | -       | -      | O     |
| Kommando MODIFY-<br>POSIX-USER-DEFAULTS    | UPD | M               | -       | O       | -       | -      | -      | E      | -       | -       | -    | -       | -       | -       | -      | O     |
| Kommando MODIFY-USER-<br>PUBSET-ATTRIBUTES | UUP | -               | -       | -       | -       | -      | -      | -      | -       | -       | -    | -       | -       | E       | -      | -     |
| Kommando MODIFY-<br>LOGON-DEFAULTS         | UDM | M               | -       | -       | -       | -      | E      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| Kommando SET-LOGON-<br>DEFAULTS            | UDS | M               | -       | -       | -       | -      | E      | -      | -       | -       | -    | -       | -       | -       | -      | -     |
| Kommando UNLOCK-<br>USER-SUSPEND           | UUS | M               | -       | -       | M       | -      | -      | -      | -       | -       | -    | -       | -       | -       | -      | -     |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                         |
|----------|-------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| catid    | *     | 0022 | Catalog identifier<br>type: c-string 1..4                                                                                                                                                                                         |
| chkmode  | *     | 0033 | Check mode<br>keywords: BATCH/DIALOG/FILE-BATCH-NCHKPASS/<br>FILE-TFT-CHKPASS/ FILE-TFT-NCHKPASS/NET-DIALOG-ACCESS/<br>OLD/OPERATOR-CONSOLE/OPERATOR-PROGRAM/<br>OPERATOR-TERMINAL/POSIX-BATCH/POSIX-REMOTE/<br>POSIX-RLOGIN/UCON |
| groupnr  | *     | 00E8 | Primary group-id of entry in POSIX group catalog<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                           |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                         |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| obj-uid  | *       | 0011 | User identifier as object<br>type: c-string 1..8                                                                                                                                                                                                                                                                                                                                  |
| oprole   | *       | 00AE | operator role<br>type: c-string 1..8                                                                                                                                                                                                                                                                                                                                              |
| parlog   | +       | 020D | /SET-LOGON-PROTECTION, /MODIFY-LOGON-PROTECTION,<br>/SET-LOGON-DEFAULTS & /MODIFY-LOGON-DEFAULTS<br>type: x-string 2..19952                                                                                                                                                                                                                                                       |
| parpos   | +       | 020E | /MODIFY-POSIX-USER-ATTRIBUTES &<br>/MODIFY-POSIX-USER-DEFAULTS<br>type: x-string 2..4800                                                                                                                                                                                                                                                                                          |
| princccl | *       | 0175 | KERBEROS client principal<br>type: c-string 1..1800 with-low                                                                                                                                                                                                                                                                                                                      |
| procnam  | *       | 0019 | Processor name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                                                                                                                                                                                                                                               |
| rejr     | *       | 005A | Reject reason<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)<br>Folgende Returncodes sind auswertbar ('x' steht für einen beliebigen Wert):<br>X'xx01xxxx' Fehlerhafte Parameterliste<br>X'xx20xxxx' Systemfehler<br>X'xx40xxxx' LOGON abgewiesen (z.B. falsches Kennwort)<br>X'xx80xxxx' LOGON wegen vorübergehendem Ressourcenengpass abgewiesen (z.B. Speichersättigung) |
| routcod  | *       | 00AD | routing code<br>type: c-string 1..3                                                                                                                                                                                                                                                                                                                                               |
| station  | *       | 0018 | Terminal name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                                                                                                                                                                                                                                                |
| uparmup  | +       | 020C | parameter list for<br>/MODIFY-USER-PUBSET-ATTRIBUTES<br>type: x-string 2..296                                                                                                                                                                                                                                                                                                     |
| uparus   | +       | 020B | parameter list for USERID add and modify<br>type: x-string 2..800                                                                                                                                                                                                                                                                                                                 |
| usern    | *       | 00AF | primary owner identification of POSIX resources<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                                                                                                                                                                            |

## Objekt UTM

| Ereignis TRM<br><br>Subcode in<br>SAT-Information<br>utmsubc | SAT-Information |         |       |       |        |         |         |         |         |         |         |         |           |         |           |           |           |         |         |        |         |         |           |         |           |           |         |         |         |           |         |       |   |
|--------------------------------------------------------------|-----------------|---------|-------|-------|--------|---------|---------|---------|---------|---------|---------|---------|-----------|---------|-----------|-----------|-----------|---------|---------|--------|---------|---------|-----------|---------|-----------|-----------|---------|---------|---------|-----------|---------|-------|---|
|                                                              | utmuser         | utmappl | lterm | pferm | muxlrm | datnam1 | datnam2 | dattype | utmacty | command | utmobj1 | utmobj2 | utmbbj3 * | utmobj4 | utmobj5 * | utmobj6 * | utmobj7 * | utmcall | applnam | tacnam | tacnaid | utuser2 | utmmode * | utmname | utmtype * | utmvers * | utmtaid | utmstat | utmreas | utmhex. * | obj-uid | user2 |   |
| Benutzeranmeldung<br>(utmsubc=SIGN)                          | M               | M       | M     | M     | O      | -       | -       | -       | -       | -       | M       | -       | O         | -       | -         | -         | -         | -       | O       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | O     | - |
| Kennwort ändern<br>(CHANGE-PW)                               | M               | M       | -     | -     | -      | -       | -       | -       | -       | -       | -       | -       | O         | -       | -         | -         | -         | -       | -       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | O     | - |
| Datenzugriff<br>(DATA ACCESS)                                | M               | M       | -     | -     | -      | M       | O       | M       | M       | -       | -       | -       | O         | -       | -         | -         | -         | -       | -       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Verwalter-Kommando<br>(ADM-CMD)                              | M               | M       | O     | O     | O      | -       | -       | -       | -       | M       | O       | O       | O         | -       | -         | -         | -         | -       | O       | O      | -       | O       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Zugriffsschlüssel ändern<br>(CHG-ACC-KEY)                    | O               | O       | -     | -     | -      | -       | -       | -       | -       | -       | -       | -       | O         | -       | -         | -         | -         | M       | -       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Teilprogramm starten<br>(START-PU)                           | M               | M       | M     | -     | -      | -       | -       | -       | -       | -       | M       | O       | O         | -       | -         | -         | -         | -       | -       | M      | M       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Teilprogramm beenden<br>(END-PU)                             | M               | M       | M     | -     | -      | -       | -       | -       | -       | -       | M       | O       | O         | -       | -         | -         | -         | -       | -       | M      | M       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Task connection zu<br>UTM-Anwendung<br>ein (TASK ON)         | -               | M       | -     | -     | -      | -       | -       | -       | -       | -       | M       | O       | O         | -       | -         | -         | -         | -       | -       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Task connection zu<br>UTM-Anwendung<br>aus (TASK OFF)        | -               | M       | -     | -     | -      | -       | -       | -       | -       | -       | M       | -       | O         | -       | -         | -         | -         | -       | -       | -      | -       | -       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Preselection- Kommando<br>(SEL-CMD)                          | M               | M       | O     | O     | -      | -       | -       | -       | -       | M       | O       | O       | O         | -       | -         | -         | -         | -       | O       | O      | -       | O       | -         | -       | -         | -         | -       | -       | -       | -         | -       | -     | - |
| Programmwechsel<br>(CHG-PROG)                                | -               | -       | -     | -     | -      | -       | -       | -       | -       | -       | -       | -       | -         | O       | O         | O         | O         | -       | -       | -      | -       | -       | O         | O       | O         | O         | O       | O       | O       | O         | -       | -     | - |
| Dynamische Appl. Erweiterung<br>(DYN-EXT)*                   | -               | -       | -     | -     | -      | -       | -       | -       | -       | -       | -       | -       | -         | O       | O         | O         | O         | -       | -       | -      | -       | -       | O         | O       | O         | O         | O       | O       | O       | O         | -       | -     | - |

\* nach dem Namen: Feld reserviert für zukünftige Erweiterungen

| <b>Feldname</b> | <b>A/I/Fil</b> | <b>exit</b> | <b>Bedeutung und Werte der Information:<br/>SDF-Datentyp oder Schlüsselwörter</b>     |
|-----------------|----------------|-------------|---------------------------------------------------------------------------------------|
| applnam         | *              | 0025        | Application name<br>type: c-string 1..8                                               |
| command         | *              | 0052        | command of utm-administrator<br>type: c-string 1..8                                   |
| datnam1         | *              | 004E        | data name for DATA-ACCESS<br>type: c-string 1..8                                      |
| datnam2         | *              | 004F        | data name for DATA-ACCESS<br>type: c-string 1..8                                      |
| dattype         | *              | 0050        | data type for DATA-ACCESS<br>keywords: G/T/U/L                                        |
| lterm           | *              | 004B        | lterm-name<br>type: c-string 1..8                                                     |
| muxlterm        | *              | 004D        | mux lterm name<br>type: c-string 1..8                                                 |
| obj-uid         | *              | 0011        | user identifier as object<br>type: c-string 1..8                                      |
| pterm           | *              | 004C        | pterm-name<br>type: c-string 1..8                                                     |
| tacnaid         | *              | 0058        | Kennzeichen<br>keywords: G/C/T/D/P                                                    |
| tacnam          | *              | 0057        | tac-name (START-PU,END-PU,ADM-CMD)<br>type: c-string 1..8                             |
| user2           | *              | 0059        | UTM user, object of CHANGE-PW<br>type: c-string 1..8                                  |
| utmacty         | *              | 0051        | for DATA-ACCESS<br>keywords: WRITE/READ/C/D                                           |
| utmappl         | *              | 0049        | application name<br>type: c-string 1..8                                               |
| utmcall         | *              | 0056        | caller's address CHANGE-ACCESS-K<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8) |
| utmhex1         | *              | 00BC        | data 1<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                           |
| utmhex2         | *              | 00BD        | data 2<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                           |
| utmhex3         | *              | 00BE        | data 3<br>type: x-string 2..16 (ALARM/FILTER: x-string 16..16)                        |

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                 |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| utmhex4  | *       | 00BF | data 4<br>type: x-string 2..16 (ALARM/FILTER: x-string 16..16)                                                                                            |
| utmmode  | *       | 00B1 | mode<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)                                                                                                 |
| utmname  | *       | 00B2 | name<br>type: c-string 1..32                                                                                                                              |
| utmobj1  | *       | 0053 | 1st object of the command<br>type: c-string 1..8                                                                                                          |
| utmobj2  | *       | 0054 | 2nd object of the command<br>type: c-string 1..8                                                                                                          |
| utmobj3  | *       | 0055 | 3rd object of the command<br>type: c-string 1..8                                                                                                          |
| utmobj4  | *       | 00B8 | 4th object of the command<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                            |
| utmobj5  | *       | 00B9 | 5th object of the command<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                            |
| utmobj6  | *       | 00BA | 6th object of the command<br>type: c-string 1..64 (ALARM/FILTER: C-string 64..64)                                                                         |
| utmobj7  | *       | 00BB | 7th object of the command<br>type: c-string 1..64 (ALARM/FILTER: C-string 64..64)                                                                         |
| utmreas  | *       | 00B7 | error code<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                           |
| utmstat  | *       | 00B6 | state<br>type: c-string 1..1                                                                                                                              |
| utmsubc  | *       | 004A | subcode for the utm event<br>keywords: CHG-ACC-KEY/ CHANGE-PW/SIGN/DATA-ACCESS/<br>ADM-CMD/START-PU/END-PU/ TASK-ON/TASK-OFF/SEL-CMD/<br>DYN-EXT/CHG-PROG |
| utmtaid  | *       | 00B5 | transaction id<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                                                                                       |
| utmtype  | *       | 00B3 | type<br>type: c-string 1..1                                                                                                                               |
| utmuser  | *       | 0048 | User Id in UTM application frame<br>type: c-string 1..8                                                                                                   |
| utmvers  | *       | 00B4 | version<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                              |

## Objekt VOLUME

| Ereignis                                    | evt | SAT-Information |        |      |      |          |       |       |        |         |         |       |         |   |
|---------------------------------------------|-----|-----------------|--------|------|------|----------|-------|-------|--------|---------|---------|-------|---------|---|
|                                             |     | volume          | newown | vsn1 | vsn2 | filename | dmsrc | share | device | devtype | inifunc | level | bakfunc |   |
| Verwalter ändert Attribute                  | VMA | M               | M      | M    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Datenträger entfernen                       | VRM | M               | -      | M    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Datenträger hinzufügen                      | VAD | M               | -      | M    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Benutzer ändert Attribute                   | VMU | M               | -      | M    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Benutzer bearbeitet Datenträger             | VVP | M               | -      | M    | -    | M        | -     | -     | -      | -       | -       | -     | -       | - |
| MAREN-Parameter ändern                      | VMM | -               | -      | -    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Datenträger Attribute anzeigen              | VSA | M               | -      | M    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| MAREN-Parameter anzeigen                    | VSP | -               | -      | -    | -    | -        | -     | -     | -      | -       | -       | -     | -       | - |
| Datenträger öffnen                          | VON | -               | -      | M    | -    | -        | M     | M     | -      | -       | -       | -     | -       | - |
| Datenträger schließen                       | VCL | -               | -      | M    | -    | -        | M     | -     | -      | -       | -       | -     | -       | - |
| geschützten Datenträger<br>initialisieren   | VIP | O               | O      | M    | M    | -        | -     | -     | M      | M       | -       | -     | -       | - |
| ungeschützten Datenträger<br>initialisieren | VIN | O               | O      | M    | M    | -        | -     | -     | M      | M       | -       | -     | -       | - |
| Platte initialisieren                       | VID | -               | -      | M    | M    | -        | -     | -     | -      | M       | M       | -     | -       | - |
| IOCF installieren                           | VIO | -               | -      | -    | -    | -        | -     | -     | -      | -       | -       | M     | -       | - |
| Datenträger anfordern (FDDRL)               | VDA | -               | -      | M    | -    | -        | -     | -     | M      | M       | -       | -     | M       | - |
| Datenträger freigeben (FDDRL)               | VDR | -               | -      | M    | -    | -        | -     | -     | M      | M       | -       | -     | M       | - |
| Datenträger ändern (FDDRL)                  | VDU | -               | -      | M    | M    | -        | -     | -     | M      | M       | -       | -     | M       | - |

| Feldname | A/F/I | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter |
|----------|-------|------|---------------------------------------------------------------------------|
| bakfunc  | *     | 0040 | Backup function (FDDRL)<br>keywords: DISK-DUMP/DISK-COPY/RL0D             |
| device   | *     | 003C | Device name<br>type: c-string 1..8                                        |
| devtype  | *     | 003D | Device type<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)          |
| dmsrc    | *     | 0004 | DMS return code<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)      |
| filename | *     | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                |
| inifunc  | *     | 003E | Initialization function (VOLIN)<br>keywords: INIT-DISK/F0RMAT-DISK        |
| level    | *     | 003F | Level # of the service processor<br>type: x-string 2..2                   |

| <b>Feldname</b> | <b>A/I/Fil</b> | <b>exit</b> | <b>Bedeutung und Werte der Information:<br/>SDF-Datentyp oder Schlüsselwörter</b> |
|-----------------|----------------|-------------|-----------------------------------------------------------------------------------|
| newown          | *              | 0038        | New volume owner<br>type: c-string 1..8                                           |
| share           | *              | 0023        | Share mode<br>keywords: SHARED/EXCLUSIVE                                          |
| volume          | *              | 0037        | Treated owner or volume owner<br>type: c-string 1..8                              |
| vsn1            | *              | 0039        | volume serial number<br>type: c-string 1..6                                       |
| vsn2            | *              | 003A        | New volume serial number<br>type: c-string 1..6                                   |

## 2.9 Tabelle der protokollierbaren Informationen (Feldnamen)

Für jedes Objekt ereignis werden bestimmte Informationen protokolliert. Diese sind im Einzelnen aus „[Tabellen der protokollierbaren Information je Objekt ereignis](#)“ auf Seite 213ff zu entnehmen.

Die folgende Tabelle zeigt in alphabetischer Ordnung die Feldnamen der protokollierbaren Information und die Werte, die diese Felder haben können.

Die Feldnamen dienen als Schlüsselwörter, mit denen die von SAT protokollierbare Information angesprochen werden kann. Sie werden in den Anweisungen //ADD-SELECTION-CONDITIONS bzw. //SELECT-RECORDS benötigt, um damit gezielt Informationen für die Aufbereitung auszuwählen.

Die Feldnamen, die auch über die Alarm-Funktion von SAT überwacht werden können oder für die eine Filterbedingung definiert werden kann, sind in der 2. Spalte (A/Fil) mit einem Stern (\*) oder Pluszeichen (+) gekennzeichnet. Mit Plus (+) gekennzeichnete Felder können nur auf ihre Existenz überprüft werden (VALUE=\*ALL). Das Kennzeichen Stern (\*) bedeutet, dass auch der Inhalt des Feldes überprüft werden kann. Falls sich der Datentyp für SAT-ALARM und SAT-FILTER von dem für SATUT unterscheidet, ist der Datentyp für SAT-ALARM und SAT-FILTER in Klammern () angegeben.

Mit dem Identifikator in der 3. Spalte kann bei Verwendung der Exit-Routine Nr.110 die SAT-Information in den protokollierten Datensätzen bearbeitet werden. Die Identifikatoren sind in sedezimaler Schreibweise angegeben.

In der letzten Spalte der Tabelle sind alle Objekte aufgeführt, bei denen der jeweilige Feldname vorkommt.

| Feldname | A/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                           | Objekte                     |
|----------|-------|------|---------------------------------------------------------------------------------------------------------------------|-----------------------------|
| access   | *     | 0006 | Open file mode<br>keywords: INPUT/REVERSE/OUTPUT/EXTEND/<br>UPDATE/INOUT/OUTIN/SINOUT/<br>INPUT-EXECUTE/UNSPECIFIED | FILE                        |
| accgrp   | *     | 0127 | Access rights for the group<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                                                    | POSIX-FILE,<br>POSIX-SYSTEM |
| acckey   | *     | 0034 | TU access key<br>type: x-string 2..2                                                                                | MEMORY POOL,<br>DATA SPACES |
| accmode  | *     | 0125 | Access mode<br>keywords:<br>READ/READ-AND-WRITE/WRITE/SEARCH                                                        | POSIX-FILE                  |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                    | Objekte                          |
|----------|---------|------|----------------------------------------------------------------------------------------------|----------------------------------|
| accoth   | *       | 0128 | Access rights for other users<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                           | POSIX-FILE,<br>POSIX-SYSTEM      |
| account  | *       | 010B | Account number<br>type: c-string 1..8                                                        | POSIX-SYSTEM                     |
| acctokb  | *       | 0070 | access mode to the key box<br>keywords:<br>OPEN-READ / OPEN-WRITE / DELETE / REPAIR          | TAPE                             |
| accusr   | *       | 0126 | Access rights for the owner<br>keywords: NONE/R/RW/RWX/RX/W/WX/X                             | POSIX-FILE<br>POSIX-SYSTEM       |
| admin    | *       | 002B | (Group)administrator identification<br>type: c-string 1..8 (user-id)                         | GROUP,<br>SPOOL DEVICE           |
| alet     | *       | 009E | access list entry token<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                 | DATA SPACES                      |
| almact   | *       | 00D6 | alarm action<br>keywords: OPERATOR-MESSAGE/<br>OPERATOR-PAUSE                                | SAT-ALARM                        |
| almlim   | *       | 00D4 | alarm time limit (in seconds)<br>type: integer -1..2 <sup>31</sup> -1                        | SAT-ALARM                        |
| almname  | *       | 00D3 | alarm name<br>type: c-string 1..8                                                            | SAT-ALARM                        |
| almrep   | *       | 00D5 | alarm repeat<br>type: integer 0..255                                                         | SAT-ALARM                        |
| almssel  | *       | 00D7 | alarm selection<br>keywords: ON/OFF                                                          | SAT-ALARM                        |
| applid   | *       | 0035 | Application identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                  | APPLICATION, BCAM                |
| appliso  | *       | 0146 | ISO name of the application<br>type: x-string 156..156<br>(ALARM/FILTER: x-string 2..156)    | BCAM                             |
| applnam  | *       | 0025 | Application name<br>type: c-string 1..8                                                      | APPLICATION,<br>BCAM, SESAM, UTM |
| appsoc   | *       | 0147 | SOCKET name of the application<br>type: x-string 156..156<br>(ALARM/FILTER: x-string 2..156) | BCAM                             |
| appluid  | *       | 0162 | Application user id<br>type: c-string 1..8                                                   | SESAM                            |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                | Objekte                                                                                               |
|----------|---------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| atflag   | *       | 0179 | Flag for file operations/events<br>keywords: NONE/AT-SYMLINK-NOFOLLOW/<br>AT-SYMLINK-FOLLOW/AT-REMOVEDIR                                                                                                                                 | POSIX-FILE                                                                                            |
| auditat  | *       | 0005 | Audit attribute<br>keywords: SUCCESS/FAILURE/ALL/NONE                                                                                                                                                                                    | ACL, FILE, PLAM                                                                                       |
| auditid  | *       | 0001 | Audit subject identification<br>type: x-string 2..32                                                                                                                                                                                     | jeder SATLOG-Satz<br>bei Einsatz von per-<br>sönlichem Logon oder<br>KERBEROS                         |
| bakfunc  | *       | 0040 | Backup function (FDDRL)<br>keywords: DISK-DUMP/DISK-COPY/RLOD                                                                                                                                                                            | VOLUME                                                                                                |
| blksize  | *       | 00CD | block size<br>type: integer, sensible values 1..32767<br>(ALARM/FILTER: integer 0..32767)                                                                                                                                                | SAT                                                                                                   |
| calend   | *       | 00F0 | calendar date for job start<br>keywords: YES/NO                                                                                                                                                                                          | JOB                                                                                                   |
| cat      | *       | 0032 | New catalog name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                                                                                                                                                        | SUBSYSTEM                                                                                             |
| catacce  | *       | 0024 | Catalog access status<br>keywords: MASTER/SLAVE                                                                                                                                                                                          | CATALOG                                                                                               |
| catid    | *       | 0022 | Catalog identifier<br>type: c-string 1..4                                                                                                                                                                                                | GUARDS, GROUP,<br>CATALOG, FILE, KEY,<br>OPERATOR-ROLE,<br>PRIVILEGE, SMS,<br>TERMINAL SET,<br>USERID |
| chkmode  | *       | 0033 | Check mode<br>keywords: BATCH/DIALOG/<br>FILE-BATCH-NCHKPASS/FILE-TFT-CHKPASS/<br>FILE-TFT-NCHKPASS/NET-DIALOG-ACCESS/<br>OLD/OPERATOR-CONSOLE/<br>OPERATOR-PROGRAM/<br>OPERATOR-TERMINAL/POSIX-BATCH/<br>POSIX-REMOTE/POSIX-RLOGIN/UCON | USERID                                                                                                |
| clmsgid  |         | 0096 | Message id. in Conslog record<br>type: c-string 1..7                                                                                                                                                                                     | CONSLOG                                                                                               |
| cloexec  | *       | 013A | Close file on exec<br>keywords: NO/YES                                                                                                                                                                                                   | POSIX-FILE                                                                                            |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Objekte           |
|----------|---------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| clorig   |         | 0098 | origin of the Conslog record<br>keywords: TPR/TU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CONSLOG           |
| clrept   |         | 0094 | Recipient<br>type: c-string 1..4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CONSLOG           |
| clsende  |         | 0095 | Sender<br>type: c-string 1..4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | CONSLOG           |
| cltext   |         | 0097 | Rest of the CONSLOG record<br>type: c-string 1..252                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CONSLOG           |
| cltype   |         | 0093 | Type of the CONSLOG record<br>type: c-string 1..39. Possible values:<br>'System message requiring a response'<br>(msg type=?)<br>'System message not requiring a response'<br>(msg type = %)<br>'Error message' (msg type = *)<br>'Emergency message' (msg type = E)<br>'Command end message' (msg type = !)<br>'Command result' (msg type = +)<br>'Additional information request' (msg type = &)<br>'Response message' (response type = R)<br>'Additional information response'<br>(response type =:)<br>'Operator command' (command type: /) | CONSLOG           |
| command  | *       | 0052 | command of utm-administrator<br>type: c-string 1..8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | UTM               |
| comread  | *       | 009D | read access protection<br>keywords: NO/YES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | DATA SPACES       |
| confnam  |         | 008B | configuration name<br>type: c-string 1..21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SAT               |
| connid   | *       | 0036 | Connection identifier<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | APPLICATION, BCAM |
| cpuid    |         | 008D | cpu identification<br>type: x-string 2..128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SAT               |
| curlim   | *       | 0117 | Current limit<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | POSIX-PROCESS     |
| curlim2  | *       | 0141 | Current limit (in multiple of 512)<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | POSIX-PROCESS     |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                 | Objekte                                                       |
|----------|---------|------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| curpid   | *       | 0100 | Current process id of the calling process<br>type: integer 0..2 <sup>31</sup> -1          | POSIX-CHILD,<br>POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM |
| currgid  | *       | 0102 | Current real POSIX group id of the calling process<br>type: integer 0..2 <sup>31</sup> -1 | POSIX-CHILD,<br>POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM |
| curruid  | *       | 0101 | Current real POSIX user id of the calling process<br>type: integer 0..2 <sup>31</sup> -1  | POSIX-CHILD,<br>POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM |
| cxtname  | *       | 000F | Context name<br>type: c-string 1..32                                                      | PROGRAM,<br>SUBSYSTEM                                         |
| databth  | *       | 0062 | data type hexa or string<br>type: x-string 2..510                                         | ANY                                                           |
| datahex  | *       | 0061 | data type hexa<br>type: x-string 2..510                                                   | ANY                                                           |
| datatxt  | *       | 0060 | data type text<br>type: c-string 1..255                                                   | ANY                                                           |
| datnam1  | *       | 004E | data name for DATA-ACCESS<br>type: c-string 1..8                                          | UTM                                                           |
| datnam2  | *       | 004F | data name for DATA-ACCESS<br>type: c-string 1..8                                          | UTM                                                           |
| dattype  | *       | 0050 | data type for DATA-ACCESS<br>keywords: G/T/U/L                                            | UTM                                                           |
| dbhconf  | *       | 0160 | DBH configuration identifier<br>type: c-string 1..1                                       | SESAM                                                         |
| dbhnam   | *       | 015F | DBH name identifier<br>type: c-string 1..1                                                | SESAM                                                         |
| dbname   | *       | 0165 | Logical database name<br>type: c-string 1..18                                             | SESAM                                                         |
| dbtable  | *       | 0167 | Table name in the catalog<br>type: c-string 1..31                                         | SESAM                                                         |
| destsup  | *       | 00A4 | destination (output support)<br>keywords: LOCAL/REMOTE/TAPE                               | SPOOL JOB                                                     |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter               | Objekte                               |
|----------|---------|------|-----------------------------------------------------------------------------------------|---------------------------------------|
| device   | *       | 003C | Device name<br>type: c-string 1..8                                                      | ADAM, SAT,<br>SPOOL DEVICE,<br>VOLUME |
| devtype  | *       | 003D | Device type<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)                        | ADAM, VOLUME                          |
| dirdes1  | *       | 0177 | File descriptor for the first directory<br>type: integer 0..2 <sup>31</sup> -1          | POSIX-FILE                            |
| dirdes2  | *       | 0178 | File descriptor for the second directory<br>type: integer 0..2 <sup>31</sup> -1         | POSIX-FILE                            |
| dltsec   | *       | 0119 | Delta seconds for adjusting the system time<br>type: integer 0..2 <sup>31</sup> -1      | POSIX-SYSTEM                          |
| dltusec  | *       | 011A | Delta microseconds for adjusting the system time<br>type: integer 0..2 <sup>31</sup> -1 | POSIX-SYSTEM                          |
| dmsrc    | *       | 0004 | DMS return code<br>type: x-string 2..4 (ALARM/FILTER: x-string 4..4)                    | FILE, VOLUME,<br>SPOOL JOBS           |
| dodvers  |         | 009A | dod version<br>type: c-string 1..7                                                      | SAT                                   |
| dpthinf  | *       | 006B | Information about the depot host<br>keywords:<br>IMPORT-PROCESS-HOST/OWN                | TAPE                                  |
| dpthost  | *       | 006D | name of the host where the transfer key box is<br>deposited<br>type: c-string 1..8      | TAPE                                  |
| dsname   | *       | 009B | data space name<br>type: c-string 1..54                                                 | DATA SPACES                           |
| egid     | *       | 0116 | Effective POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                         | POSIX-PROCESS                         |
| eltname  | *       | 0008 | Element name<br>type: c-string 1..64                                                    | PLAM, PROGRAM,<br>SPOOL JOBS          |
| eltype   | *       | 000A | Element type<br>type: c-string 1..8                                                     | PLAM, PROGRAM,<br>SPOOL JOBS          |
| eltvers  | *       | 0009 | Element version<br>type: c-string 1..24                                                 | PLAM, PROGRAM,<br>SPOOL JOBS          |
| enamprc  | *       | 001E | ENAMP return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                  | MEMORY POOL                           |
| enctype  | *       | 0174 | KERBEROS encryption type<br>type: integer 0..2 <sup>31</sup> -1                         | KEY                                   |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                   | Objekte                                                                                |
|----------|---------|------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| endreas  | *       | 0017 | End reason<br>keywords: ABEND/CANCEL/LOGOFF/<br>MOVE-JOBS/SHUTDOWN                          | JOB                                                                                    |
| endtype  | *       | 0016 | Job termination status<br>keywords: NORMAL/ABNORMAL                                         | JOB                                                                                    |
| erase    | *       | 0041 | File deletion status<br>keywords: YES/NO                                                    | SPOOL JOBS                                                                             |
| errno    | *       | 0103 | POSIX error number<br>type: integer $-2^{31}..2^{31}-1$                                     | POSIX-CHILD<br>POSIX-PROCESS<br>POSIX-FILE<br>POSIX-SYSTEM                             |
| euid     | *       | 0113 | Effective POSIX user id<br>type: integer $0..2^{31}-1$                                      | POSIX-PROCESS                                                                          |
| evitnam  | *       | 002F | Eventing/serialization item name<br>type: c-string 1..64<br>(ALARM/FILTER: c-string 64..64) | EVENTING ITEM                                                                          |
| evt      |         | 00F3 | Event-type id<br>type: c-string 1..3                                                        | jeder SATLOG-Satz                                                                      |
| evtaud   | *       | 00CE | event auditability<br>keywords: SUCCESS/FAILURE/ALL/NONE                                    | SAT                                                                                    |
| fappend  | *       | 0136 | Append to the end of file<br>keywords: NO/YES                                               | POSIX-FILE                                                                             |
| fcreat   | *       | 0137 | Create file<br>keywords: NO/YES                                                             | POSIX-FILE                                                                             |
| fctcmd   | *       | 012D | File control operation<br>keywords: DUP-FILDES/SET-FILDES-FLAGS/<br>SET-FILMODE-FLAGS       | POSIX-FILE                                                                             |
| fildes   | *       | 010C | File descriptor<br>type: integer $0..2^{31}-1$                                              | POSIX-FILE                                                                             |
| filename | *       | 0003 | File name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                  | ACL, FILE, PLAM,<br>POSIX-FILE,<br>PROGRAM, SPOOL<br>JOBS, SAT, SYNTAX<br>FILE, VOLUME |
| filpos   | *       | 011B | Offset in mapped file (in multiple of 512)<br>type: integer $0..2^{31}-1$                   | POSIX-FILE                                                                             |
| flush    | *       | 0014 | Job removal<br>keywords: YES/NO                                                             | JOB                                                                                    |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                            | Objekte                                                          |
|----------|---------|------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| fnocTTY  | *       | 0139 | No controlling terminal<br>keywords: NO/YES                                                          | POSIX-FILE                                                       |
| fnpatrn  | *       | 0063 | filename pattern<br>type: c-string 1..80                                                             | FILE, SPOOL JOBS                                                 |
| fparcat  | +       | 0208 | Parameter List File<br>Type: x-string 2..12000                                                       | FILE                                                             |
| fract    | *       | 00FA | Filter Action Logging on/off<br>keywords: NO-RECORDING/RECORDING                                     | SAT-FILTER                                                       |
| ftrname  | *       | 00FB | Filter Name<br>Type: c-string 1..8                                                                   | SAT-FILTER                                                       |
| ftrsel   | *       | 00FC | Filter selection<br>keywords: OFF/ON                                                                 | SAT-FILTER                                                       |
| ftrunc   | *       | 0138 | Truncate file length to 0<br>keywords: NO/YES                                                        | POSIX-FILE                                                       |
| gid      | *       | 0114 | POSIX group id<br>type: integer 0..2 <sup>31</sup> -1                                                | POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM                    |
| gparadu  | +       | 0209 | Parameter list for add group<br>type: x-string 2..5000                                               | GROUP                                                            |
| gparmdu  | +       | 0210 | Parameter list for modify group<br>type: x-string 2..10000                                           | GROUP                                                            |
| gparmod  | +       | 0201 | Modify parameter list<br>type: x-string 2..1860                                                      | GUARDS                                                           |
| gparrem  | +       | 0202 | delete parameter list<br>type: x-string 2..432                                                       | GUARDS                                                           |
| groupid  | *       | 0002 | Group subject identification (user-group)<br>type: c-string 1..8                                     | jeder SATLOG-Satz<br>bei Einsatz von SRPM                        |
| groupnr  | *       | 00E8 | Primary group-id of entry in POSIX group catalog<br>type: integer 0..2 <sup>31</sup> -1              | USERID                                                           |
| guard    | *       | 009F | Guard name<br>type: c-string 1..40                                                                   | FITC, GUARDS,<br>COOWNER<br>PROTECTION,<br>DEFAULT<br>PROTECTION |
| homedir  | *       | 0108 | Home directory of a user<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255) | POSIX-SYSTEM                                                     |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter           | Objekte                           |
|----------|---------|------|-------------------------------------------------------------------------------------|-----------------------------------|
| hostnam  | *       | 0029 | Name of the host<br>type: c-string 1..8                                             | APPLICATION,<br>BCAM, SESAM, TAPE |
| infile   | *       | 00E5 | information file<br>type: c-string 1..54 (ALARM/FILTER: filename)                   | SUBSYSTEM                         |
| inifunc  | *       | 003E | Initialization function (VOLIN)<br>keywords: INIT-DISK/FORMAT-DISK                  | VOLUME                            |
| intdate  | *       | 000D | Internal date<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                  | PROGRAM                           |
| intime   | *       | 001A | Time of the job spoolin<br>type: c-string 1..14<br>(ALARM/FILTER: c-string 14..14)  | JOB                               |
| intname  | *       | 000B | Internal name<br>type: c-string 1..41                                               | PROGRAM                           |
| intvers  | *       | 000C | Internal version<br>type: c-string 1..24                                            | PROGRAM                           |
| ipv4own  | *       | 014A | Own IP address (format V4)<br>type: c-string 7..15                                  | BCAM, IPSEC                       |
| ipv4ptn  | *       | 014B | Partner IP address (format V4)<br>type: c-string 7..15                              | BCAM, IPSEC                       |
| ipv6own  | *       | 014C | Own IP address (format V6)<br>type: c-string 39..39                                 | BCAM, IPSEC                       |
| ipv6ptn  | *       | 014D | Partner IP address (format V6)<br>type: c-string 39..39                             | BCAM, IPSEC                       |
| itslown  | *       | 0151 | Own ISO-TSEL<br>type: x-string 64..64<br>(ALARM/FILTER: x-string 2..64)             | BCAM                              |
| itslptn  | *       | 0152 | Partner ISO-TSEL<br>type: x-string 64..64<br>(ALARM/FILTER: x-string 2..64)         | BCAM                              |
| jobcmd   | *       | 00A7 | job command origin<br>keywords: PRINT                                               | SPOOL JOB                         |
| jobcopy  | *       | 00A8 | copies number<br>type: integer 0..255                                               | SPOOL JOB                         |
| joberrt  | *       | 00AA | detected errors during spoolout<br>keywords: DEVICERR/DMS/<br>NONE/PLAM/SYSTEM/USER | SPOOL JOB                         |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                               | Objekte       |
|----------|---------|------|---------------------------------------------------------------------------------------------------------|---------------|
| joborig  | *       | 00A6 | job origin<br>keywords: NORMAL/RTCOPY/RTDIRECT                                                          | SPOOL JOB     |
| jobpage  | *       | 00A9 | printed pages number<br>type: integer 0..2 <sup>31</sup> -1                                             | SPOOL JOB     |
| jobterm  | *       | 00A5 | Termination or interruption type<br>keywords: ABORT/CANCEL/KEEP<br>NORMAL/RESPPOOL/SUSPEND              | SPOOL JOB     |
| jobtype  | *       | 0012 | Job type<br>keywords: ENTR = ENTER job<br>TASK = subtask,<br>MOVE-JOBS = import job description         | JOB           |
| jvname   | *       | 005B | Job variable-name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                      | JOB VARIABLES |
| jvpatrn  | *       | 005E | Job variable-pattern<br>type: c-string 1..80                                                            | JOB VARIABLES |
| jvsrc    | *       | 005D | Return-code of Job Variables<br>x-string 2..4 (ALARM/FILTER: x-string 4..4)                             | JOB VARIABLES |
| keepopt  | *       | 0047 | Keep option<br>keywords: YES/NO                                                                         | PLAM          |
| keybox   | *       | 0066 | Key box name<br>type: c-string 1..54                                                                    | TAPE          |
| keyid    | *       | 0067 | Identification string for the encryption key<br>type: c-string 1..18<br>(ALARM/FILTER: c-string 18..18) | TAPE          |
| kvno     | *       | 0175 | KERBEROS key version number<br>type: integer 0..2 <sup>31</sup> -1                                      | KEY           |
| ldata    | +       | 0203 | General hexa fields<br>type: x-string 2..64000                                                          | ANY           |
| ldvers   | *       | 0099 | Load unit version<br>type: c-string 1..24                                                               | PROGRAM       |
| level    | *       | 003F | Level # of the service processor<br>type: x-string 2..2                                                 | VOLUME        |
| libname  | *       | 00A0 | object module library<br>type: c-string 1..54 (ALARM/FILTER: filename)                                  | SUBSYSTEM     |
| linknam  | *       | 0107 | Link name<br>type: type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)             | POSIX-FILE    |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter          | Objekte                     |
|----------|---------|------|------------------------------------------------------------------------------------|-----------------------------|
| loaduni  | *       | 000E | Load unit name<br>type: c-string 1..32                                             | PROGRAM                     |
| logquan  | *       | 00F9 | sign for logging quantity<br>type: c-string 1..8                                   | SAT                         |
| lterm    | *       | 004B | lterm-name<br>type: c-string 1..8                                                  | UTM                         |
| mapaddr  | *       | 011C | Memory address of the mapping<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8) | POSIX-FILE                  |
| maplen   | *       | 011D | Length of the mapped area<br>type: integer 0..2 <sup>31</sup> -1                   | POSIX-FILE                  |
| mapprot  | *       | 0129 | Access permission for the mapped pages<br>keywords: NONE/R/RW/RWX/RX/W/WX/X        | POSIX-FILE                  |
| mapshar  | *       | 012A | Visibility of write accesses to the mapped pages<br>keywords: PRIVATE/SHARED       | POSIX-FILE                  |
| maxlim   | *       | 0118 | Maximum limit<br>type: integer 0..2 <sup>31</sup> -1                               | POSIX-PROCESS               |
| maxlim2  | *       | 0142 | Maximum limit (in multiple of 512)<br>type: integer 0..2 <sup>31</sup> -1          | POSIX-PROCESS               |
| memclas  | *       | 0020 | memory class of the memory pool<br>keywords: CLASS3/CLASS4/CLASS5/CLASS6           | MEMORY POOL,<br>PROGRAM     |
| mempool  | *       | 001C | memory pool name<br>type: c-string 1..54                                           | MEMORY POOL,<br>PROGRAM     |
| mempriv  | *       | 0021 | Privilege of the mem. pool pages<br>keywords: YES/NO                               | DATA SPACES,<br>MEMORY POOL |
| msgfile  | *       | 00E4 | message file<br>type: c-string 1..54 (ALARM/FILTER: filename)                      | SUBSYSTEM                   |
| muxlrm   | *       | 004D | mux lterm name<br>type: c-string 1..8                                              | UTM                         |
| newcat   | *       | 00EC | New or merged catalog identification<br>type: c-string 1..4                        | CATALOG                     |
| newfdes  | *       | 010D | New file descriptor<br>type: integer 0..2 <sup>31</sup> -1                         | POSIX-FILE                  |
| newfile  | *       | 0007 | New file name<br>type: c-string 1..54 (ALARM/FILTER: filename)                     | FILE, SAT                   |
| newjv    | *       | 005C | New job variable name<br>type: c-string 1..54 (ALARM/FILTER: filename)             | JOB VARIABLES               |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                    | Objekte                                         |
|----------|---------|------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| newown   | *       | 0038 | New volume owner<br>type: c-string 1..8                                                                      | VOLUME                                          |
| newpath  | *       | 0106 | New name of file resp. directory<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255) | POSIX-FILE                                      |
| newvset  | *       | 00D9 | New volume set name<br>type: c-string 1..4                                                                   | SMS                                             |
| nsems    | *       | 0123 | Total number of all semaphores<br>type: integer 0..2 <sup>31</sup> -1                                        | POSIX-SYSTEM                                    |
| nwelnam  | *       | 0042 | New/base element name<br>type: c-string 1..64                                                                | PLAM                                            |
| nweltyp  | *       | 0044 | New/base element type<br>type: c-string 1..8                                                                 | PLAM                                            |
| nwelve   | *       | 0043 | New/base element version<br>type: c-string 1..24                                                             | PLAM                                            |
| nwguard  | *       | 00AB | new guard name<br>type: c-string 1..24                                                                       | GUARDS                                          |
| nwrlnam  | *       | 00C1 | New name of protection rule<br>type: c-string 1..12                                                          | COOWNER<br>PROTECTION,<br>DEFAULT<br>PROTECTION |
| nwtssnam | *       | 00C6 | Name of new terminal set<br>type: c-string 1..8                                                              | TERMINAL SET                                    |
| nwtssown | *       | 00C8 | Owner of new terminal set<br>type: c-string 1..8                                                             | TERMINAL SET                                    |
| nwtssscp | *       | 00C7 | Scope of new terminal set<br>keyword: GROUP / SYSTEM / USER                                                  | TERMINAL SET                                    |
| obj-evt  | *       | 00C9 | event as object<br>type: c-string 1..3 (ALARM/FILTER: c-string 3..3)                                         | SAT-ALARM                                       |
| obj-fld  | *       | 00D8 | object field<br>type: c-string 1..7                                                                          | SAT-ALARM                                       |
| obj-gid  | *       | 002A | Group identifier as object<br>type: c-string 1..8                                                            | GROUP                                           |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                         | Objekte                                                                                      |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| obj-uid  | *       | 0011 | User identifier as object<br>type: c-string 1..8                                                                                  | JOB, KEY,<br>PRIVILEGE,<br>OPERATOR ROLE,<br>SAT, SUBSYSTEM,<br>USERID, UTM,<br>POSIX-SYSTEM |
| objname  | *       | 00C2 | Name of object<br>type: c-string 1..54                                                                                            | COOWNER<br>PROTECTION,<br>DEFAULT<br>PROTECTION                                              |
| oprole   | *       | 00AE | operator role<br>type: c-string 1..8                                                                                              | OPERATOR ROLE,<br>USERID                                                                     |
| parcra   | +       | 0215 | Parameter list for add coowner prot rule<br>type: x-string 2..384                                                                 | COOWNER<br>PROTECTION                                                                        |
| parcrm   | +       | 0216 | Parameter list for modify coowner prot rule<br>type: x-string 2..384                                                              | COOWNER<br>PROTECTION                                                                        |
| pardaa   | +       | 020F | Parameter list for add default prot attributes<br>type: x-string 2..312                                                           | DEFAULT<br>PROTECTION                                                                        |
| pardam   | +       | 0210 | Parameter list for modify default prot attributes<br>type: x-string 2..352                                                        | DEFAULT<br>PROTECTION                                                                        |
| pardra   | +       | 0213 | Parameter list for add default prot rule<br>type: x-string 2..424                                                                 | DEFAULT<br>PROTECTION                                                                        |
| pardrm   | +       | 0214 | Parameter list for modify default prot rule<br>type: x-string 2..424                                                              | DEFAULT<br>PROTECTION                                                                        |
| pardua   | +       | 0211 | Parameter list for add default prot uid<br>type: x-string 2..952                                                                  | DEFAULT<br>PROTECTION                                                                        |
| pardur   | +       | 0212 | Parameter list for remove default prot uid<br>type: x-string 2..952                                                               | DEFAULT<br>PROTECTION                                                                        |
| parkrbp  | +       | 0219 | Parameter list for add/modify KERBEROS principal<br>type: x-string 2..280                                                         | KEY                                                                                          |
| parlog   | +       | 020D | /SET-LOGON-PROTECTION,<br>/MODIFY-LOGON-PROTECTION,<br>/SET-LOGON-DEFAULTS &<br>/MODIFY-LOGON-DEFAULTS<br>type: x-string 2..19952 | USERID                                                                                       |
| parpos   | +       | 020E | /MODIFY-POSIX-USER-ATTRIBUTES &<br>/MODIFY-POSIX-USER-DEFAULTS<br>type: x-string 2..4800                                          | USERID                                                                                       |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                | Objekte                       |
|----------|---------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| partiso  | *       | 0148 | ISO name of the partner<br>type: x-string 156..156<br>(ALARM/FILTER: x-string 2..156)                                                                                                                                                                                    | BCAM                          |
| partnam  | *       | 0026 | Partner name<br>type: c-string 1..8                                                                                                                                                                                                                                      | APPLICATION, BCAM             |
| partsb   | +       | 0217 | Parameter list for build terminal set<br>type: x-string 2..200                                                                                                                                                                                                           | TERMINAL SET                  |
| partsm   | +       | 0218 | Parameter list for modify terminal set<br>type: x-string 2..6800                                                                                                                                                                                                         | TERMINAL SET                  |
| partsoc  | *       | 0149 | SOCKET name of the partner<br>type: x-string 156..156<br>(ALARM/FILTER: x-string 2..156)                                                                                                                                                                                 | BCAM                          |
| parttyp  | *       | 0028 | Type of the partner<br>keywords: APPLICATION/TERMINAL                                                                                                                                                                                                                    | APPLICATION                   |
| pathnam  | *       | 0105 | Name of file resp. directory<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255)                                                                                                                                                                 | POSIX-PROCESS,<br>POSIX-FILE  |
| periodd  | *       | 00EA | number of day for action repetition<br>type: integer 0..255                                                                                                                                                                                                              | SAT                           |
| periodh  | *       | 00EB | number of hours for action repetition<br>type: integer 0..255                                                                                                                                                                                                            | SAT                           |
| pgid     | *       | 0110 | Process group id<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                                                                                                  | POSIX-PROCESS                 |
| pid      | *       | 010F | Process id<br>type: integer 0..2 <sup>31</sup> -1                                                                                                                                                                                                                        | POSIX-CHILD,<br>POSIX-PROCESS |
| pidrecv  | *       | 010E | Process id of receiving process<br>type: integer -2 <sup>31</sup> ..2 <sup>31</sup> -1                                                                                                                                                                                   | POSIX-PROCESS                 |
| plamrc   | *       | 0046 | PLAM return code<br>type: c-string 1..13<br>(ALARM/FILTER: x-string 16..16)<br>Format: zzzz/xxxxxxx<br>zzzz = Primärkode (Dezimal)<br>xxxxxxx= Sekundärkode (Sedezimal)<br>Mit /HELP-MSG PLAzxxx kann Information über<br>den entsprechenden Returncode abgerufen werden | PLAM,<br>SPOOL DEVICE         |
| port     | *       | 00B0 | port name<br>type: c-string 1..54                                                                                                                                                                                                                                        | FITC                          |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                   | Objekte                                       |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| portown  | *       | 014E | Own port number<br>type: integer 0..65535                                                                                                                                   | BCAM                                          |
| portptn  | *       | 014F | Partner port number<br>type: integer 0..65535                                                                                                                               | BCAM                                          |
| prexit   | *       | 00D0 | Exit routine activated<br>keywords: YES/NO                                                                                                                                  | SAT                                           |
| priallo  | *       | 00CB | primary allocation<br>type: integer $-2^{31}..2^{31}-1$                                                                                                                     | SAT                                           |
| princl   | *       | 0172 | KERBEROS client principal<br>type: c-string 1..1800 with-low<br>(ALARM/FILTER: c-string 1..255 with-low)                                                                    | KEY, USERID                                   |
| princsv  | *       | 0173 | KERBEROS server principal<br>type: c-string 1..1800 with-low<br>(ALARM/FILTER: c-string 1..255 with-low)                                                                    | KEY                                           |
| priv     | *       | 002D | Processed privilege identification<br>keywords:<br>siehe „Tabelle der Privilegien“ im Handbuch<br>„SECOS - Security Control System - Zugangs- und<br>Zugriffskontrolle“ [1] | PRIVILEGE                                     |
| privset  | *       | 00A3 | privilege set name<br>type: c-string 1..8                                                                                                                                   | PRIVILEGE                                     |
| procnam  | *       | 0019 | Processor name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                                         | JOB, USERID,<br>SPOOL DEVICE,<br>POSIX-SYSTEM |
| pswdpar  | *       | 0064 | password parameter<br>keywords: YES/NO                                                                                                                                      | FILE                                          |
| pterm    | *       | 004C | pterm-name<br>type: c-string 1..8                                                                                                                                           | UTM                                           |
| pthtnam  | *       | 0027 | Name of the partner host<br>type: c-string 1..8                                                                                                                             | APPLICATION, BCAM                             |
| pwcmd    | *       | 0130 | Suboperation for event XPW (set user attributes)<br>keywords: FORK-WITH-USER-CHANGE/<br>MOD-POSIX-USER-ATTR/<br>POSIX-RLOGIN-ACCESS                                         | POSIX-SYSTEM                                  |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Objekte                  |
|----------|---------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| rc       | *       | 003B | fdbk return code<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)<br>Beim Objekt IPSEC sind folgende Returncodes auswertbar:<br><ul style="list-style-type: none"> <li>– X'00400106' unzulässiger Wert für SPI (Security Parameter Index)</li> <li>– X'00400206' ungültige Signatur</li> <li>– X'00400306' Fehlermeldung der Cryptobox: Entschlüsselung schlug fehl</li> <li>– X'00400406' Signatur/Verschlüsselung erforderlich</li> <li>– X'00400506' 1. Security Association für Input erforderlich, aber nicht verfügbar</li> <li>– X'00400606' 2. Security Association für Input erforderlich, aber nicht verfügbar</li> <li>– X'00400706' Unzulässiger Security Protokoll-Header</li> </ul> | APPLICATION, BCAM, IPSEC |
| reason   | *       | 008C | reason<br>keywords: RESUME-SAT-LOGGING/CHANGE-SAT-FILE/DMS-ERROR/HOLD-SAT-LOGGING/PERIODIC-SWITCHING/SHUTDOWN/STARTUP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SAT                      |
| rejr     | *       | 005A | Reject reason<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)<br>Folgende Returncodes sind auswertbar ('x' steht für einen beliebigen Wert):<br><ul style="list-style-type: none"> <li>– X'xx01xxxx' Fehlerhafte Parameterliste</li> <li>– X'xx20xxxx' Systemfehler</li> <li>– X'xx40xxxx' LOGON abgewiesen (z.B. falsches Kennwort)</li> <li>– X'xx80xxxx' LOGON wegen vorübergehendem Ressourcenengpass abgewiesen (z.B. Speichersättigung)</li> </ul>                                                                                                                                                                                                                                         | USERID                   |
| rejreas  | *       | 001B | Reject reason<br>keywords: INV-AUTHORIZATION/SYSTEM-ERROR/CMD-PARAM-ERROR/SATURATION/NO-ERROR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | JOB                      |
| repeat   | *       | 0015 | Job start period<br>keywords: YES/NO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | JOB                      |
| repfile  | *       | 00A1 | rep file name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | SUBSYSTEM                |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                              | Objekte                                                       |
|----------|---------|------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| rerun    | *       | 0013 | Job reinitiation<br>keywords: YES/NO                                                                                   | JOB                                                           |
| res      |         | 00F5 | Event result<br>keywords: F/S                                                                                          | jeder SATLOG-Satz                                             |
| resjoin  | *       | 0045 | user-catalog lost or not<br>keywords: YES/NO                                                                           | CATALOG                                                       |
| resourc  | *       | 012C | Resource<br>keywords: CPU-TIME/FILE-SIZE/NO-OF-FILES                                                                   | POSIX-PROCESS                                                 |
| retval   | *       | 0104 | POSIX return value<br>type: integer $-2^{31}..2^{31}-1$                                                                | POSIX-CHILD,<br>POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM |
| rgid     | *       | 0115 | Real POSIX group id<br>type: integer $0..2^{31}-1$                                                                     | POSIX-PROCESS                                                 |
| routcod  | *       | 00AD | routing code<br>type: c-string 1..3                                                                                    | OPERATOR ROLE,<br>USERID                                      |
| ruid     | *       | 0112 | Real POSIX user id<br>type: integer $0..2^{31}-1$                                                                      | POSIX-PROCESS                                                 |
| rule     | *       | 00CA | rule<br>keywords: FILES-BY-EVENT/<br>INDEPENDENT/UNCHANGED                                                             | SAT                                                           |
| rulenam  | *       | 00C0 | Name of protection rule<br>type: c-string 1..20                                                                        | COOWNER<br>PROTECTION,<br>DEFAULT<br>PROTECTION               |
| savpar   | *       | 00D1 | saved parameters<br>keywords: ALARM/FILTER/<br>LOGGING-FILE-ATTRIBUTES/PRESELECTION/<br>SAT-SUPPORT                    | SAT                                                           |
| savval   | *       | 00D2 | saved value<br>keywords: CURRENT/STANDARD                                                                              | SAT                                                           |
| schema   | *       | 0166 | Schema name in the catalog<br>type: c-string 1..31                                                                     | SESAM                                                         |
| scope    | *       | 001D | Eventing/serialization item scope<br>Memory pool scope<br>keywords: LOCAL/GROUP/GLOBAL/<br>USER-GROUP/UNDEFINED/SYSTEM | DATA SPACES,<br>EVENTING ITEM,<br>MEMORY POOL,<br>PROGRAM     |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                                                                                                                                                                                                                                                                                                                                                                    | Objekte                     |
|----------|---------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| sdevrdo  | *       | 013D | Symbolic device is read only<br>keywords: NO/YES                                                                                                                                                                                                                                                                                                                                                                                                                                             | POSIX-FILE                  |
| sdfcmd   | *       | 00AC | SDF command name<br>type: c-string 1..30                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SYNTAX FILE                 |
| secallo  | *       | 00CC | secondary allocation<br>type: integer $-2^{31}..2^{31}-1$                                                                                                                                                                                                                                                                                                                                                                                                                                    | SAT                         |
| semact   | *       | 0133 | Action code for semaphore control operation<br>keywords: REMOVE-ID/SET-OPTIONS                                                                                                                                                                                                                                                                                                                                                                                                               | POSIX-SYSTEM                |
| semcmd   | *       | 0131 | Semaphore control operation<br>keywords: CONTROL/GET                                                                                                                                                                                                                                                                                                                                                                                                                                         | POSIX-SYSTEM                |
| semid    | *       | 0121 | Id of the semaphore<br>type: integer $0..2^{31}-1$                                                                                                                                                                                                                                                                                                                                                                                                                                           | POSIX-SYSTEM                |
| semnum   | *       | 0122 | Number of a specific semaphore<br>type: integer $0..2^{31}-1$                                                                                                                                                                                                                                                                                                                                                                                                                                | POSIX-SYSTEM                |
| sessubc  | *       | 015E | Subcode for the SESAM events<br>type: c-string 1..4<br>Abhängig vom jeweiligen Event sind folgende Sub-<br>codes auswertbar:<br><b>Event SET</b><br>– STRT: Start of a SESAM-DBH-Task<br>– END: End of a SESAM-DBH-Task<br><b>Event SEU</b><br>– END: End of a session<br><b>Event SEA</b><br>– ADM Administration stmt<br><b>Event SEP</b><br>– USR: Add/remove/modify users<br>– PRI: Grant/revoke rights<br><b>Event SES</b><br>– DDL: DDL stmt<br>– SSL: SSL stmt<br>– UTI: Utility stmt | SESAM                       |
| sestext  | *       | 0168 | Additional information for the SESAM events<br>type: c-string 1..64                                                                                                                                                                                                                                                                                                                                                                                                                          | SESAM                       |
| setpcmd  | *       | 012E | Suboperation for event XSP (set process group id)<br>keywords: SET-PGID/SET-SID/<br>SET-SID-AND-PGID                                                                                                                                                                                                                                                                                                                                                                                         | POSIX-PROCESS               |
| setsgid  | *       | 013C | Set the set-group-id bit<br>keywords: NO/YES                                                                                                                                                                                                                                                                                                                                                                                                                                                 | POSIX-FILE,<br>POSIX-SYSTEM |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                   | Objekte                     |
|----------|---------|------|---------------------------------------------------------------------------------------------|-----------------------------|
| setsuid  | *       | 013B | Set the set-user-id bit<br>keywords: NO/YES                                                 | POSIX-FILE,<br>POSIX-SYSTEM |
| share    | *       | 0023 | Catalog shareability<br>Share mode<br>keywords: SHARED/EXCLUSIVE                            | CATALOG,<br>VOLUME          |
| shell    | *       | 0109 | Shell of a user<br>type: c-string 1..1024 with-low<br>(ALARM/FILTER: posix-pathname 1..255) | POSIX-SYSTEM                |
| shmact   | *       | 0134 | Action code for shared memory control operation<br>keywords: REMOVE-ID/SET-OPTIONS          | POSIX-SYSTEM                |
| shmaddr  | *       | 011E | Address of the shared memory<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)           | POSIX-SYSTEM                |
| shmcmd   | *       | 0132 | Shared memory control operation<br>keywords: ATTACH/CONTROL/DETACH/GET                      | POSIX-SYSTEM                |
| shmid    | *       | 0120 | Id of the shared memory<br>type: integer 0..2 <sup>31</sup> -1                              | POSIX-SYSTEM                |
| shmrdo   | *       | 013E | Shared memory is read only<br>keywords: NO/YES                                              | POSIX-SYSTEM                |
| shmsize  | *       | 011F | Size of the shared memory<br>type: integer 0..2 <sup>31</sup> -1                            | POSIX-SYSTEM                |
| shortid  | *       | 001F | Short memory pool name<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                 | MEMORY POOL                 |
| signal   | *       | 012B | Signal sent to a process<br>keywords: ABORT/KILL                                            | POSIX-PROCESS               |
| sopact   | *       | 0065 | SPACEOPT action code<br>keywords: CLEAR-VOL/REDUCE-EXT/<br>START-JOB                        | FILE                        |
| spid     | *       | 009C | Space identifier<br>type: x-string 2..16<br>(ALARM/FILTER: x-string 16..16)                 | DATA SPACES                 |
| srchost  | *       | 006F | Host from which the key box is accessed<br>type: c-string 1..8                              | TAPE                        |
| srctsn   | *       | 0071 | TSN of the accessing subject<br>type: c-string 1..4                                         | TAPE                        |
| srcuser  | *       | 0072 | Userid of the accessing subject<br>type: c-string 1..8                                      | TAPE                        |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                      | Objekte                      |
|----------|---------|------|----------------------------------------------------------------------------------------------------------------|------------------------------|
| sscmd    | *       | 00E7 | DSSM commands permission<br>Keywords: ALLOWED/BY-ADMINISTRATOR/<br>FORBIDDEN                                   | SUBSYSTEM                    |
| sshld    | *       | 00E6 | Indicates if subsystem can be deleted / held<br>Keywords: ALLOWED/FORBIDDEN                                    | SUBSYSTEM                    |
| station  | *       | 0018 | Terminal name<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                             | JOB, USERID,<br>SPOOL DEVICE |
| stmtctf  | *       | 0164 | Number of unsuccessful statements in the session<br>type: integer 0..2 <sup>31</sup> -1                        | SESAM                        |
| stmtcts  | *       | 0163 | Number of successful statements in the session<br>type: integer 0..2 <sup>31</sup> -1                          | SESAM                        |
| storcla  | *       | 00ED | storage class<br>type: c-string 1..8                                                                           | SMS                          |
| subcod   | *       | 005F | subcode<br>type: c-string 1..4                                                                                 | ANY                          |
| subsnam  | *       | 0030 | Name of the subsystem<br>type: c-string 1..8                                                                   | SUBSYSTEM                    |
| subsver  | *       | 0031 | Version of the subsystem<br>type: c-string 1..7                                                                | SUBSYSTEM                    |
| suppar   | *       | 013F | name of SAT support parameter<br>keywords: POSIX-EVENTS                                                        | SAT                          |
| supval   | *       | 0140 | value of SAT support parameter<br>keywords: DISABLED / ENABLED                                                 | SAT                          |
| symbdev  | *       | 010A | Symbolic device name (/dev/disk/nnnn)<br>type: c-string 1..14 with-low<br>(ALARM/FILTER: posix-pathname 1..14) | POSIX-FILE                   |
| synfile  | *       | 00A2 | syntax file name<br>type: c-string 1..54 (ALARM/FILTER: filename)                                              | SYNTAX FILE,<br>SUBSYSTEM    |
| syntype  | *       | 002E | Syntax file type<br>keywords: SYSTEM/GROUP/SUBSYSTEM/USER                                                      | SYNTAX FILE                  |
| sysid    |         | 0088 | system-id<br>type: c-string 1..3                                                                               | SAT, SUBSYSTEM               |
| sysnam   |         | 0089 | system-name<br>type: c-string 1..8                                                                             | SAT, SUBSYSTEM               |
| sysvers  |         | 008A | system version<br>type: c-string 1..4                                                                          | SAT, SUBSYSTEM               |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter     | Objekte                                       |
|----------|---------|------|-------------------------------------------------------------------------------|-----------------------------------------------|
| tacnaid  | *       | 0058 | Kennzeichen<br>keywords: G/C/T/D/P                                            | UTM                                           |
| tacnam   | *       | 0057 | tac-name (START-PU,END-PU,ADM-CMD)<br>type: c-string 1..8                     | UTM                                           |
| tgthost  | *       | 0068 | Name of target host<br>type: c-string 1..8                                    | TAPE                                          |
| tgtkbox  | *       | 0069 | Name of target key box<br>type: c-string 1..54                                | TAPE                                          |
| timestp  |         | 00F1 | Time (date and time of the record creation)<br>Format: yyyy-mm-dd/hh:mm:ss    | jeder SATLOG-Satz                             |
| trfkbox  | *       | 006A | Name of transfer key box<br>type: c-string 1..54                              | TAPE                                          |
| tsn      |         | 00F4 | TSN subject<br>type: c-string 1..4                                            | jeder SATLOG-Satz                             |
| tsn-inf  | *       | 0010 | TSN object<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)               | JOB, FITC,<br>SPOOL JOBS                      |
| tsname   | *       | 00C3 | Terminal set name<br>type: c-string 1..8                                      | TERMINAL SET                                  |
| tsowner  | *       | 00C5 | Terminal set owner<br>type: c-string 1..8                                     | TERMINAL SET                                  |
| tsscope  | *       | 00C4 | Terminal set scope<br>keyword: GROUP / SYSTEM / USER                          | TERMINAL SET                                  |
| uaudef   |         | 00FD | Default of user audit attribute<br>keywords: OFF/ON                           | SAT                                           |
| uid      | *       | 0111 | POSIX user id<br>type: integer 0..2 <sup>31</sup> -1                          | POSIX-PROCESS,<br>POSIX-FILE,<br>POSIX-SYSTEM |
| ulimcmd  | *       | 012F | Suboperation for event XLM (set process limits)<br>keywords: SET-FILE-LIMIT   | POSIX-PROCESS                                 |
| uparmup  | +       | 020C | parameter list for<br>/MODIFY-USER-PUBSET-ATTRIBUTES<br>type: x-string 2..296 | USERID                                        |
| uparus   | +       | 020B | parameter list for USERID add and modify<br>type: x-string 2..800             | USERID                                        |
| upper    | *       | 002C | Upper group identification<br>type: c-string 1..8                             | GROUP                                         |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter               | Objekte           |
|----------|---------|------|-----------------------------------------------------------------------------------------|-------------------|
| user-id  |         | 00F6 | user subject identification<br>type: c-string 1..8 (user-id)                            | jeder SATLOG-Satz |
| useraud  | *       | 00CF | user auditability<br>keywords: YES/NO                                                   | SAT               |
| userkey  | *       | 0143 | User-selected numerical key<br>type : integer $-2^{31}..2^{31}-1$                       | POSIX-SYSTEM      |
| usernr   | *       | 00AF | primary owner identification of POSIX resources<br>type: integer $0..2^{31}-1$          | USERID            |
| user2    | *       | 0059 | UTM user, object of CHANGE-PW<br>type: c-string 1..8                                    | UTM               |
| utmacty  | *       | 0051 | for DATA-ACCESS<br>keywords: WRITE/READ/C/D                                             | UTM               |
| utmappl  | *       | 0049 | application name<br>type: c-string 1..8                                                 | UTM               |
| utmcall  | *       | 0056 | caller's address CHANGE-ACCESS-KEY<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8) | UTM               |
| utmhex1  | *       | 00BC | data 1<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                             | UTM               |
| utmhex2  | *       | 00BD | data 2<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                             | UTM               |
| utmhex3  | *       | 00BE | data 3<br>type: x-string 2..16<br>(ALARM/FILTER: x-string 16..16)                       | UTM               |
| utmhex4  | *       | 00BF | data 4<br>type: x-string 2..16<br>(ALARM/FILTER: x-string 16..16)                       | UTM               |
| utmmode  | *       | 00B1 | mode<br>type: c-string 1..4 (ALARM/FILTER: c-string 4..4)                               | UTM               |
| utmname  | *       | 00B2 | name<br>type: c-string 1..32                                                            | UTM               |
| utmobj1  | *       | 0053 | 1st object of the command<br>type: c-string 1..8                                        | UTM               |
| utmobj2  | *       | 0054 | 2nd object of the command<br>type: c-string 1..8                                        | UTM               |
| utmobj3  | *       | 0055 | 3rd object of the command<br>type: c-string 1..8                                        | UTM               |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/I/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter                                                                           | Objekte    |
|----------|---------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| utmobj4  | *       | 00B8 | 4th object of the command<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                      | UTM        |
| utmobj5  | *       | 00B9 | 5th object of the command<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                      | UTM        |
| utmobj6  | *       | 00BA | 6th object of the command<br>type: c-string 1..64<br>(ALARM/FILTER: c-string 64..64)                                                                | UTM        |
| utmobj7  | *       | 00BB | 7th object of the command<br>type: c-string 1..64<br>(ALARM/FILTER: c-string 64..64)                                                                | UTM        |
| utmreas  | *       | 00B7 | error code<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                     | UTM        |
| utmsct   | *       | 0161 | UTM session counter<br>type: x-string 2..16 (ALARM/FILTER: x-string 16..16)                                                                         | SESAM      |
| utmstat  | *       | 00B6 | state<br>type: c-string 1..1                                                                                                                        | UTM        |
| utmsubc  | *       | 004A | subcode for the utm event<br>keywords: CHG-ACC-KEY/ CHANGE-PW/ SIGN/DATA-ACCESS/ADM-CMD/START-PU/ END-PU/TASK-ON/TASK-OFF/SEL-CMD/ DYN-EXT/CHG-PROG | UTM        |
| utmtaid  | *       | 00B5 | transaction id<br>type: x-string 2..8 (ALARM/FILTER: x-string 8..8)                                                                                 | UTM        |
| utmtype  | *       | 00B3 | type<br>type: c-string 1..1                                                                                                                         | UTM        |
| utmuser  | *       | 0048 | User id in UTM application frame<br>type: c-string 1..8                                                                                             | SESAM, UTM |
| utmvers  | *       | 00B4 | version<br>type: c-string 1..8 (ALARM/FILTER: c-string 8..8)                                                                                        | UTM        |
| volkind  | *       | 006E | Kind of volumes for which the key can be used<br>resp. for which the encryption attributes are modified<br>keywords:<br>FROM-FOREIGN-MAREN-DOMAIN   | TAPE       |
| volset   | *       | 00EF | volume set<br>type: c-string 1..4                                                                                                                   | SMS        |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

| Feldname | A/Fil | exit | Bedeutung und Werte der Information:<br>SDF-Datentyp oder Schlüsselwörter | Objekte                    |
|----------|-------|------|---------------------------------------------------------------------------|----------------------------|
| volume   | *     | 0037 | Treated owner or volume owner<br>type: c-string 1..8                      | VOLUME                     |
| vslist   | *     | 00EE | volume set list<br>type: c-string 1..8                                    | SMS                        |
| vsn1     | *     | 0039 | volume serial number<br>type: c-string 1..6                               | FILE, SAT, TAPE,<br>VOLUME |
| vsn2     | *     | 003A | New volume serial number<br>type: c-string 1..6                           | VOLUME                     |

Tabelle 5: Protokollierbare Information: Feldnamen, Werte und Objekte

---

# Fachwörter

Die folgende Übersicht enthält Definitionen bzw. Erläuterungen zu Begriffen, die in diesem Handbuch im Zusammenhang mit den Funktionseinheiten verwendet werden.

## **Abrechnungsnummer**

Account Number

Sie bezeichnet ein Abrechnungskonto für die zugehörige Benutzerkennung. Eine Abrechnungsnummer kann mehreren Benutzerkennungen zugewiesen werden; eine Benutzerkennung kann über mehrere (bis zu 60) Abrechnungsnummern verfügen. Die Abrechnungsnummer wird bei SET-LOGON-PARAMETERS (oder LOGON) und ENTER-JOB ausgewertet.

## **Ämterhäufung**

Function Accumulation

Soll eine Benutzerkennung auf einem Pubset als Gruppenverwalter bestimmt werden (ADD/MODIFY-USER-GROUP), so wird das Kommando zurückgewiesen, wenn die Benutzerkennung das Recht „systemglobale Benutzerverwaltung“ auf diesem Pubset oder auf dem Home-Pubset besitzt. Soll einer Benutzerkennung auf einem Pubset das Recht „systemglobale Benutzerverwaltung“ zugewiesen werden (SET-PRIVILEGE), so wird dies zurückgewiesen, wenn die Benutzerkennung auf diesem Pubset Verwalter einer Benutzergruppe ist.

## **Attributguard**

Attribute Guard

Spezielles *Guard*, in dem Standardwerte für Schutzattribute von Objekte festgelegt werden.

## **Authentisierung**

Authentication

Nachweis einer angegebenen Identität.

## **BACL**

siehe *Einfache Zugriffskontrollliste*

### **Benutzer**

User

Er wird von einer Benutzerkennung repräsentiert. Der Begriff Benutzer ist ein Synonym für Personen, Anwendungen, Verfahren etc., die über eine Benutzerkennung Zugang zum Betriebssystem erhalten können.

### **Benutzerattribute**

User Attribute

Alle Merkmale einer Benutzerkennung, die im Benutzerkatalog hinterlegt sind.

### **Benutzergruppe**

User Group

Eine Benutzergruppe ist die Zusammenfassung einzelner Benutzer und hat einen Namen (Benutzergruppenkennung).

### **Benutzergruppeneintrag**

Group Entry

Sätze im Benutzerkennungskatalog (ehemals \$TSOS.TSOSJOIN, neuer Name siehe *Benutzerkennungskatalog*), die die Daten für eine Benutzergruppe enthalten.

### **Benutzergruppenkennung**

Group Identificaton

Name einer Benutzergruppe, der beim Einrichten der Benutzergruppe vergeben wird. Über die Benutzergruppenkennung wird die Benutzergruppe angesprochen.

### **Benutzerkatalog**

siehe *Benutzerkennungskatalog*

### **Benutzerkennung (USER-ID)**

User Identification

Ist ein maximal acht Zeichen langer Name und wird im Benutzerkatalog eingetragen.

Anhand der Benutzerkennung wird der Benutzer beim Systemzugang identifiziert. Alle Dateien und Jobvariablen werden unter einer Benutzerkennung eingerichtet. Die Namen der Dateien und Jobvariablen werden mit der Benutzerkennung im Dateikatalog hinterlegt.

### **Benutzerkennungskatalog**

User ID catalog

Datei \$TSOS.SYSSRPM, die die Benutzerattribute aller Benutzerkennungen eines Pubsets enthält.

Synonym: Benutzerkatalog

### **Benutzerkommando**

User Command

Kommandos, die unter einer beliebigen Benutzerkennung im Systemmodus (/) oder auch im Programm-Modus mit CMD-Makros gegeben werden können.

### **Benutzerorganisation**

User organization

Die Zusammenfassung von Benutzerkennungen zu Benutzergruppen. Hierdurch wird die Nachbildung bestehender Organisationsformen ebenso gestattet wie die projektorientierte Zusammenfassung von Benutzern.

### **Benutzerrechte**

User Privilege

Alle an eine Benutzerkennung vergebenen und im Benutzerkennungskatalog hinterlegten Attribute, die Rechte darstellen.

### **Benutzerverwaltung**

User Administration

siehe *Systemglobale Benutzerverwaltung*

### **Beweissicherung**

Audit

Grundfunktion eines sicheren Systems; Protokollierung von Abläufen und Aufbereitung der protokollierten Daten.

### **CONSLOG-Datei**

CONSLOG file

Protokolldatei, in der der gesamte Nachrichtenverkehr zwischen Bedienstationen, berechtigten Benutzerprogrammen und dem System aufgezeichnet wird.

### **Co-owner Protection**

siehe *Miteigentümerschutz*

### **Dateikatalog**

File Directory

Datei, die auf jedem Pubset vorhanden ist (in SM-Pubsets auf jedem Volumenset). Jede Datei und jede Jobvariable eines Pubsets sind im entsprechenden Dateikatalog eingetragen. Dateien von Privatplatten und Bändern können im Dateikatalog eingetragen sein.

Ein Katalogeintrag enthält alle Attribute (Schutzattribute, Lage der verwalteten Daten usw.) einer Datei bzw. einer Jobvariablen.

### **Datenschutz**

#### Data Protection

Im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, durch den Schutz der personenbezogenen Daten vor Mißbrauch bei der Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

Im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Mißbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

- Datenschutz wird im Unternehmen realisiert durch
- Einhaltung von Unternehmensgrundsätzen und Unternehmensrichtlinien,
- Einhaltung von gesetzlichen Vorschriften,
- problembewußtes Handeln,
- zweckentsprechende Anwendung der Datensicherung.

### **Datensicherung**

#### Data Security

Technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten; d.h. insbesondere zu erreichen, dass

- der Zugriff zu Daten nur Berechtigten möglich ist,
- keine unerwünschte bzw. unberechtigte Verarbeitung von Daten erfolgt,
- die Daten bei der Verarbeitung nicht verfälscht werden,
- die Daten reproduzierbar sind.

Diese Aufgabe wird gelöst durch

- in Hardware und Software enthaltene technische und organisatorische Vorkehrungen und Maßnahmen,
- übrige organisatorische sowie bauliche und personelle Vorkehrungen und Maßnahmen.

### **Datensichtstation**

#### Terminal

E/A-Gerät, bestehend aus Tastatur und Bildschirm, das über Netzsoftware dem Verarbeitungsrechner (VAR) angeschlossen ist.

Die Datensichtstation kann dem VAR direkt (über MSN) angeschlossen sein oder sie kann eine Komponente eines Kommunikationsrechners sein (Adressierung über Stations- bzw. Transportsystemadresse).

### **Default Protection**

siehe *Standardschutz*

## Eigentümer

Owner

Benutzerkennung, unter der ein *Objekt* eingerichtet ist

## Einfache Zugriffskontrollliste BACL

Basic Access Control List BACL

Einträge im Dateikatalog, die die Zugriffsrechte auf Dateien und Jobvariable für den Eigentümer, die Benutzergruppe und alle anderen Benutzerkennungen für Lesen, Schreiben und Ausführen regeln.

## Filter

Mechanismus zur Verfeinerung der Preselection von SAT

## First-Start

Beim First-Start werden Systemdateien neu eingerichtet. Vom System werden eine Reihe von Benutzerkennungen vergeben (z.B. TSOS, SYSPRIV, SYSDUMP, SERVICE, SYSGEN, SYSNAC, SYSHSMS, SYSUSER, SYSSNAP, SYSSPOOL, SYSAUDIT). Beim First-Start wird immer der Benutzerkennungskatalog angelegt.

Beim First-Start für einzelne Pubsets sind zwei Varianten möglich: Entweder Systemstart mit diesem Pubset oder IMCAT-Processing (logisches Hinzufügen eines weiteren Pubsets).

## Frist

siehe *Schutzfrist*

## Funktionalitätsklasse

Functionality Class

Klasse, die bestimmte Mindestanforderungen bezüglich der Funktionalität der Sicherheitsfunktionen an ein System der Informationstechnik stellt.

Die Funktionalitätsklassen sind definiert innerhalb der „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)“, 1. Fassung vom 11. Januar 1989, herausgegeben von der Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung.

## Gemeinschaftlicher Datenspeicherbereich

Public Space

Benannter Plattenspeicherbereich, der für eine definierte Anzahl von Benutzerkennungen des Betriebssystems verfügbar ist. Dieser Speicherbereich kann sich über einen oder mehrere Pubsets erstrecken.

## Gruppenkennung

siehe *Benutzergruppenkennung*

### **Gruppenmitglied**

Group Member

Benutzerkennung, die einer Benutzergruppe zugeordnet ist. Der Gruppenverwalter kann einem Gruppenmitglied im Rahmen des Gruppenpotentials Betriebsmittel zuweisen.

### **Gruppenpotential**

Enthält alle Betriebsmittel und Rechte, die an eine Benutzergruppe gebunden sind und an die Gruppenmitglieder der Benutzergruppe bzw. an hierarchisch untergeordnete Benutzergruppen vergeben werden können.

### **Gruppenverwalter**

Group Administrator

Ein Benutzer, der Gruppenpotentiale, Gruppenmitglieder und die untergeordnete Gruppenstruktur verwalten kann. Die Benutzerkennung, unter der diese Tätigkeiten ausgeführt werden dürfen, ist im Gruppenpotential der jeweiligen Benutzergruppe hinterlegt.  
Benutzerkennung, die mit dem Gruppenverwalterrecht ausgestattet ist.

### **Gruppenverwalterrecht**

Group Administrator Privilege

Berechtigt eine Benutzerkennung zur Verwaltung von

- den Benutzerkennungen der eigenen Benutzergruppe und
- hierarchisch untergeordneten Benutzerkennungen sowie
- hierarchisch untergeordneten Benutzergruppen.

Das Gruppenverwalterrecht kann in drei Ausprägungen vergeben werden, die den Umfang der erlaubten Tätigkeiten festlegen, diese sind:

- Manage Resources
- Manage Members
- Manage Groups.

### **Guard**

Schutzprofil, das mit dem Schutzmechanismus *GUARDS* erstellt und verwaltet werden kann.

### **GUARDS**

Generally Usable Access Control Administration System

Universeller Schutzmechanismus für Objekte im BS2000.

### **Identifizierung**

Identification

Verfahren zur Erkennung einer Person oder eines *Objekts*.

### **Installation**

Vorgang des Bereitstellens von Gerätetechnik und Software  
Bei einem Benutzer vorhandene Gerätetechnik und Software.

### **IT-Sicherheitskriterien**

siehe *Sicherheitskriterien*

### **Katalogkennung**

Catalog Identification CATID

Kennzeichnet einen Pubset durch maximal 4 Zeichen <cat-id 1...4>.

### **Kennwort**

Password

Folge von Zeichen, die der Benutzer eingeben muss, um den Zugriff zu einer Benutzerkennung, einer Datei, einer Jobvariablen, einem Netzknoten oder einer Anwendung zu erhalten.

Das Benutzerkennungs-Kennwort dient zur Authentifizierung des Benutzers. Es dient dem Zugangsschutz. Das Datei-Kennwort dient zur Überprüfung der Zugriffsberechtigung beim Zugriff auf eine Datei (Jobvariable). Es dient dem Zugriffsschutz.

Synonym: Passwort

### **Kommandoprofil**

Command Profile

siehe *Profile*

### **Miteigentümer**

Co-owner

Benutzerkennung, die vom *Eigentümer* eines *Objekts* berechtigt wird, sein *Objekt* mitzuverwalten.

### **Miteigentümerschaft**

Co-ownership

Berechtigung, fremde *Objekte* mitzuverwalten

### **Miteigentümerschutz**

Co-owner Protection

Spezieller Zugriffsschutz für *Objekte*, die von fremden Benutzerkennungen mitverwaltet werden dürfen

### **Miteigentümerschutzregel**

Co-Owner Protection Rule

*Regel*, die für ein oder mehrere *Objekte* bestimmt, welche Bedingungen eine Benutzerkennung erfüllen muss, um *Miteigentümer* dieser *Objekte* zu sein.

### **Objekt**

Object

Passives Element eines DV-Systems, das Daten enthält oder aufnimmt und auf das eine Operation wie Lesen, Schreiben, Ausführen u.ä. angewendet werden kann.

Beispiele: Dateien, Jobvariablen, Benutzerkennungen, *Terminal-Sets*

### **offline-Betrieb**

Arbeitsweise einer funktionellen Einheit, wenn sie nicht unter der direkten Steuerung eines Rechners steht.

Weder gesteuert noch verbunden mit einem Rechner (Gegensatz zu online-Betrieb).

### **online-Betrieb**

Arbeitsweise einer funktionellen Einheit, wenn sie unter der direkten Steuerung eines Rechners steht.

Fähigkeit eines Benutzers zur interaktiven Arbeit mit einem Rechner.

Benutzerzugriff zu einem Rechner über eine Datensichtstation.

Gesteuert von oder verbunden mit einem Rechner (Gegensatz zu offline-Betrieb)

### **Operator-Role**

Zusammenfassung einer Menge von Routing-Codes unter einem Namen.

Es sind beliebige Kombinationen der 40 Routing-Codes möglich.

### **Personenbezogene Beweissicherung**

Personal Audit for Individual Accountability

Nachvollziehbarkeit des Umgangs mit einem System.

Identifikation entweder in Form: eine Benutzerkennung entspricht einem

Benutzer oder ein Benutzer darf ausschließlich eine Bedienstation benutzen.

### **persönliche Identifizierung**

Für eine Benutzerkennung können andere Benutzerkennungen als zusätzlich zugangsberechtigt festgelegt werden. Während der Dialogzugangsprüfung wird eine personenspezifische Identifizierung/Authentisierung veranlasst. Die Benutzerkennung, die mit der personenbezogenen Identifizierung angegeben wurde, wird in die SAT-Einträge übernommen. Somit ist es möglich, Personen als Urheber einzelner Aktionen auch nachträglich zu ermitteln.

### **Privilegienverwalter**

siehe *Sicherheitsbeauftragter*

**Privileg**

Privilege

Systemglobales Recht, das zur Ausführung bestimmter Kommandos und zum Aufruf bestimmter Programmschnittstellen berechtigt (z.B. SECURITY-ADMINISTRATION)

**Profil**

Profile

Ein einer Benutzererkennung zugeordneter Kommando-Vorrat, dessen Zulässigkeit über Syntax-Dateien sichergestellt wird.

**Pubset**

Pubset

Durch eine Katalogkennung (Catid) definierte Menge von gemeinschaftlichen Plattenspeicher-Einheiten.

Man unterscheidet Single-Feature-Pubsets (SF-Pubsets) und System-Managed-Pubset (SM-Pubset).

Ein SF-Pubset besteht aus einer oder mehreren Platten, die in den wesentlichen Eigenschaften (Plattenformat, Allokierungseinheit, Verfügbarkeit) übereinstimmen müssen.

Ein SM-Pubset kann im Gegensatz dazu aus mehreren so genannten Volume-Sets mit unterschiedlichen Eigenschaften bestehen. Nur innerhalb eines Volume-Sets müssen die wesentlichen Eigenschaften der Platten übereinstimmen.

**Qualitätsstufe**

Assurance Level

Hierarchische Unterteilung bezüglich der Qualität eines Systems der Informationstechnik (IT-Systems). Bei der Evaluation wird die Qualität eines IT-Systems bewertet. Anhand dieser Bewertung erfolgt eine Einstufung in eine der Qualitätsstufen Q0 bis Q7.

**Regel**

Rule

Eintrag in einem *Regelbehälter*.

Abhängig von ihrem Zweck unterscheidet man *Miteigentümerschutzregeln* und *Standardschutzregeln*.

**Regelbehälter**

Rule Container

Spezielles Guard zur Aufnahme von *Miteigentümerschutzregeln* oder den *Standardschutzregeln*.

### **Rolle**

Role

Gruppierung von Attributen, die einem Subjekt zugeordnet werden können, z.B. Sicherheitsbeauftragter.

### **Sammelprivileg**

Privilege-Set

Zusammenfassung systemglobaler Privilegien zu einer Gruppe, die mit einem selbstgewählten Namen bezeichnet wird.

### **SAT**

Security Audit Trail

Protokollierung sicherheitsrelevanter Ereignisse

### **SATLOG-Datei**

SATLOG file

SAT-Protokolldatei, in der SATCP sicherheitsrelevante Ereignisse aufgezeichnet.

### **Schutzattribute**

Security Attributes

Sicherheitsrelevante Eigenschaften eines Objekts, die Art und potenzielle Möglichkeit des Zugriffs auf dieses Objekt festlegen.

Für Dateien gibt es folgende Schutzattribute: ACCESS/USER-ACCESS, SERVICE-bit, AUDIT-Attribut (NONE/SUCCESS/FAILURE/ALL), RDPASS, WRPASS, EXPASS, RETPD, BACL und GUARD.

### **Schutzfrist**

Retention Period

Zeitintervall, in dem ein Objekt (Datei) nicht verändert oder gelöscht werden kann.

### **SF-Pubset**

Single-Feature-Pubset siehe *Pubset*

### **SHUTDOWN**

Vorgang der geordneten Systembeendigung (einschließlich des Sicherns spezieller Systemdateien).

### **Sichere Hardware-Konfiguration**

Installierte Gerätetechnik (einschließlich Datenfernübertragungstechnik und Netz), die keinen Sicherheitseinschränkungen unterliegt.

### **Sicheres BS2000**

BS2000, das aktiv entsprechend der F2/Q3-Sicherheitsanforderungen konfiguriert wurde.

Synonyme Begriffe dazu sind: „F2/Q3-System“ oder „evaluiertes System“. Das Gegenteil eines „sicheren BS2000“ ist nicht ein „unsicheres BS2000“, sondern ein System, das beispielsweise nicht-bewertete Teile enthält oder das nicht den Kriterien F2/Q3 entspricht bzw. ein System, das nicht gemäß der empfohlenen Konfiguration betrieben wird.

### **Sicherheitsbeauftragter**

Security Administrator, Security Officer

Sicherheitsbeauftragter im herkömmlichen Sinne: Organisatorisch-administrative Institution.

Die Kennung des Sicherheitsbeauftragten kann mit Hilfe des STARTUP-PARAMETER-SERVICE festgelegt werden. Bei Auslieferung ist die Kennung des Sicherheitsbeauftragten SYSPRIV. Der Sicherheitsbeauftragte hat das Recht, systemglobale Privilegien an Benutzerkennungen zu vergeben und zu entziehen. Er hat das Recht, die SAT-Protokollierung aus- und einzuschalten, Operator-Roles zu verwalten sowie Benutzerkennungen und Ereignisse für die Protokollierung auszuwählen.

### **Sicherheitskriterien**

Security Criteria

Dienen der Bewertung der Sicherheit von Systemen der Informationstechnik.

Sie bestehen aus Funktionalitätsklassen und Qualitätsstufen.

Dies wird in Form von Fx/Qty (Funktionalitätsklasse x und Qualitätsstufe y) dargestellt; Beispiel: F2/Q3 bedeutet Funktionalitätsklasse 2 und Qualitätsstufe 3.

### **Sicherheitsverwalter**

siehe *Sicherheitsbeauftragter*

### **Single Sign On**

Mechanismus, der es ermöglicht nach einmaliger Identifizierung/Authentisierung Zugang zu verschiedenen Rechnern und Anwendungen zu erhalten. Dieser Zugang wird über Zertifikate gesteuert.

### **Single-Feature-Pubset**

siehe *Pubset*

### **SM-Pubset**

System-Managed-Pubset siehe *Pubset*

### **SMS**

System-Managed-Storage  
Konzept für die Pubset-Verwaltung.

### **SRPM**

System Resources and Privileges Management  
Betriebsmittel und Privilegien werden im BS2000 gewöhnlich von der Kennung TSOS verwaltet. SRPM erlaubt, diese Aufgaben auch für andere Benutzerkennungen zuzulassen, die Aufgaben also zu verteilen.

### **Standardschutz**

Default Protection  
Schutzmechanismus, mit dem Standardwertvorgaben für Schutzattribute vorgenommen werden können.

### **Standardschutzregel**

Default Protection Rule  
*Regel*, die für ein oder mehrere *Objekte* bestimmt, welche Schutzattribute diese *Objekte* standardmäßig erhalten.

### **Subjekt**

Subject  
Aktives Element eines DV-Systems, von dem eine Operation wie Lesen, Schreiben, Ausführen u.ä. ausgehen kann, die einen Informationsfluss bewirkt oder den Systemzustand ändert, z.B. Kennung, Programm, Programmteil.

### **System-Managed-Pubset**

siehe *Pubset*

### **Systemeinleitung**

STARTUP  
Laden der Betriebssystem-Software. Es wird unterschieden in:  
– DIALOG-STARTUP  
– FAST-STARTUP  
– AUTOMATIC-STARTUP  
Die Varianten der Systemeinleitung unterscheiden sich durch unterschiedlichen Automatisierungsgrad.

### **Systemglobale Benutzerverwaltung**

User Administration  
Sie umfasst die Verwaltung von Benutzerkennungen und Benutzergruppen bezüglich Betriebsmitteln und Benutzerrechten, das Neueinrichten, Modifizieren und Löschen von Benutzerkennungen und Benutzergruppen.

### **Systemglobale Privilegien**

Alle mit dem Kommando /SET-PRIVILEGE vergebaren Rechte sowie das Recht des Sicherheitsbeauftragten und das Recht der Kennung TSOS. Diese sind im Einzelnen im Abschnitt „Privilegien der Systemverwaltung“ aufgezählt. *Systemglobale Privilegien* und *Systemverwalterrechte* sind identisch.

### **Systemlauf**

Session

Vorgänge/Aktivitäten zwischen Systemeinleitung und Systembeendigung.

### **Systemressourcen**

System Resource

Ein Betriebsmittel eines Rechnersystems, das von einem Job oder einer Task angefordert bzw. freigegeben werden kann.

### **Systemverwalterrechte**

siehe *Systemglobale Privilegien*

### **Systemverwaltung**

System Administration

Struktureinheit im Rechenzentrum

Personenkreis, der Benutzerkennungen verwendet, an die systemglobale Rechte gebunden sind.

### **Terminal-Set**

Terminal-Sets haben den Zweck, die Menge der Datensichtstationen, über die der Dialogzugang zu einer Benutzerkennung möglich ist, effektiv verwalten zu können. In einem Terminal-Set wird eine Liste von voll- oder teilqualifizierten Datensichtstationsnamen zusammengefasst.

### **Zugangsklasse**

Access Class

Es werden in SECOS folgende Zugangsklassen unterschieden:

|                      |                                                  |
|----------------------|--------------------------------------------------|
| DIALOG-ACCESS        | (Zugang vom Teilnehmersystem)                    |
| NET-DIALOG-ACCESS    | (Dialog-Zugang aus dem Netz)                     |
| BATCH-ACCESS         | (Zugang für Batchaufträge vom gleichen Rechner)  |
| OPERATOR-ACCESS-TERM | (Operating-Betrieb)                              |
| OPERATOR-ACCESS-PROG | (Operating-Betrieb für programmierte Operatoren) |
| OPERATOR-ACCESS-CONS | (Konsol-Zugang)                                  |

|                     |                                |
|---------------------|--------------------------------|
| POSIX-RLOGIN-ACCESS | (POSIX-Remote-Login)           |
| POSIX-REMOTE-ACCESS | (POSIX-Remote-Kommando-Zugang) |

### **Zugangsschutz**

Beinhaltet alle Methoden zum Schutz eines DV-Systems vor unberechtigtem Systemzugang.

### **Zugriffsberechtigter**

Authorized User

Subjekt, das auf ein Objekt zugreifen darf, z.B. Benutzererkennung auf Datei.

### **Zugriffsberechtigung**

Access Admission

Legt fest, welches Subjekt auf welche Weise auf ein Objekt zugreifen darf.

### **Zugriffsrecht**

Access Right

Recht eines Subjekts, auf ein Objekt mit einem vorgegebenen Zugriffsrecht zugreifen zu dürfen.

### **Zugriffsschutz**

Zugriffsschutz bezeichnet die Regeln, nach denen in einem DV-System Subjekte auf Objekte zugreifen können, und die Methoden, mit denen die Einhaltung dieser Regeln sichergestellt werden kann.

### **Zugriffstyp**

Access Type

Allgemein: Legt fest, wie auf ein Objekt zugegriffen werden kann.

Die Zugriffstypen für Dateien sind Lesen, Schreiben und Ausführen.

Die Zugriffstypen für Jobvariablen sind Lesen und Schreiben.

Der Zugriffstyp für Memory Pools ist das Anschließen an den Memory Pool (ENAMP).

Der Zugriffstyp für die Serialization ist das Anschließen an die Serialisierungskennung (ENASI).

Der Zugriffstyp für die Ereignissteuerung ist das Anschließen an die ereignisgesteuerte Verarbeitung (ENAEI).

Synonym: Zugriffsart

---

# Literatur

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

- [1] **SECOS**  
**Security Control System - Zugangs- und Zugriffskontrolle**  
Benutzerhandbuch
- [2] **BS2000 OSD/BC**  
**Einführung in die Systembetreuung**  
Benutzerhandbuch
- [3] **BS2000 OSD/BC**  
**Systeminstallation**  
Benutzerhandbuch
- [4] **BS2000 OSD/BC**  
**Kommandos**  
Benutzerhandbuch
- [5] **ARCHIVE (BS2000)**  
Benutzerhandbuch
- [6] **BS2000 OSD/BC**  
**Einführung in das DVS**  
Benutzerhandbuch
- [7] **BS2000 OSD/BC**  
**DVS-Makros**  
Benutzerhandbuch
- [8] **EDT (BS2000)**  
**Anweisungen**  
Benutzerhandbuch
- [9] **FDDRL (BS2000)**  
Benutzerhandbuch

- [10] **openFT für BS2000**  
**Enterprise File Transfer in der offenen Welt**  
Benutzerhandbuch
- [11] **FTAC-BS2000 (BS2000)**  
Erweiterter Zugangsschutz für File-Transfer  
Benutzerhandbuch
- [12] **HSMS (BS2000)**  
**Hierarchisches Speicher Management System**  
**Band 1: Funktionen, Verwaltung und Installation**  
Benutzerhandbuch
- [13] **HSMS (BS2000)**  
**Hierarchisches Speicher Management System**  
**Band 2: Anweisungen**  
Benutzerhandbuch
- [14] **BS2000 OSD/BC**  
**Dienstprogramme**  
Benutzerhandbuch
- [15] **BS2000 OSD/BC**  
**Makroaufrufe an den Ablaufteil**  
Benutzerhandbuch
- [16] **MAREN (BS2000)**  
**Bandverwaltung in BS2000**  
Benutzerhandbuch
- [17] **openUTM (BS2000, UNIX, Windows)**  
**Anwendungen generieren**  
Benutzerhandbuch
- [18] **BS2000 OSD/BC**  
**System Exits**  
User Guide
- [19] **SDF (BS2000)**  
**Dialogschnittstelle SDF**  
Benutzerhandbuch
- [20] **openSM2 (BS2000)**  
**Software Monitor**  
Band 1: Verwaltung und Bedienung

- 
- [21] **VM2000**  
**Virtuelles Maschinensystem**  
Benutzerhandbuch
  - [22] **LMS (BS2000)**  
SDF-Format  
Benutzerhandbuch
  - [23] **SDF-P (BS2000)**  
**Programmieren in der Kommandosprache**  
Benutzerhandbuch
  - [24] **POSIX (BS2000)**  
Grundlagen für Anwender und Systemverwalter  
Benutzerhandbuch
  - [25] **POSIX (BS2000)**  
**Kommandos**  
Benutzerhandbuch
  - [26] **C-Bibliotheksfunktionen (BS2000)**  
für POSIX-Anwendungen  
Referenzhandbuch
  - [27] **SPOOL (BS2000)**  
Teil 1, Benutzerhandbuch
  - [28] **SPOOL (BS2000)**  
Teil 2, Dienstprogramme  
Benutzerhandbuch
  - [29] **BS2000 OSD/BC**  
**Migration Guide**  
Benutzerhandbuch
  - [30] **PROP-XT (BS2000)**  
Programmiertes Operating mit komfortablen Sprachmitteln von SDF-P  
Produktthandbuch
  - [31] **JV (BS2000)**  
**Jobvariablen**  
Benutzerhandbuch

- [32] **BS2000 OSD/BC**  
**System Managed Storage**  
Benutzerhandbuch
- [33] **SESAM/SQL-Server (BS2000)**  
**Datenbankbetrieb**  
Benutzerhandbuch

## Sonstige Literatur

Diese Literatur kann nicht über Fujitsu Technology Systems bezogen werden.

- [34] **IT-Sicherheitskriterien:** Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)

Herausgegeben von der ZSI, Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung, 1. Fassung vom 11. Januar 1989. - Köln: Bundesanzeiger, 1989  
ISBN 3-88784-192-1

---

# Stichwörter

\*EXTENDED-Feld 25

\*LNG-Feld 51

## A

Abrechnung

Account Number 303

Nummer 303

Access

Admission 316

Class 315

Right 316

Type 316

ADAM, Objekt 216

ADD-SAT-ALARM-CONDITIONS (SAT-Kommando) 60

ADD-SAT-FILTER-CONDITIONS (SAT-Kommando) 68

ADD-SELECTION-CONDITIONS (SATUT-Anweisung) 148

Admission

Access 316

Alarm

aktivieren 39

ändern 80

Anwendungshinweis 66

anzeigen 124

definieren 60

Einführung 8

Funktion 38

Grundeinstellungen 42

Kommandos 38

Konsole 38

löschen 116

maximale Zahl 66

MODIFY-SAT-ALARM-CONDITIONS 80

online 38

REMOVE-SAT-ALARM-CONDITIONS 116

SHOW-SAT-ALARM-CONDITIONS 124

sichern 38

speichern 38, 121

Ämterhäufung 303

Analyse, SAT-Datei 143

analysis-file

Analyseergebnisse ablegen 143

SAVE-SELECTED-RECORDS 156

Verwendungszweck 142, 143

Zusatzinformationen 142

ANY, Objekt 216

APPLICATION, Objekt 217

Archivierung, SAT-Datei 142

Assurance Level 311

Audit 305

Audit-Attribut 21

Ereignis 22

EVENT 22

Objekt 23

Subjekt 21

USER 21

Aufbereitung, Bedingungen 140

Aufbereitungsbedingung

Beispiele 153

Bereich 149

Bestandteile 148

Feldnamen 150

festlegen 163

suchen 149

vergleichen 150

Verknüpfung 148

### Auswahl

- aktueller Stand 21
- durch den Benutzer 23
- durch den Sicherheitsbeauftragten 21
- Gültigkeitsdauer 21
- Kriterien 21
- Protokoll 16
- Standard-Werte 106
- Voreinstellung 22

### Auswahl-Regeln

- ändern 106
- FILES-BY-EVENTS 25
- Grundregel 24
- INDEPENDENT-Logik 24
- SAT 21

### Auswahl-Werte

- RESUME-SAT-LOGGING 26

### auswerten

- Dateimanipulationen 36
- Empfehlungen 36
- Umfang 158
- UTM-Ereignisse 37

### Auswertungslauf 142

### Authentication 303

### Authentisierung 303

### Authorized User 316

## B

### BACL 307

### Basic Access Control List (BACL) 307

### BCAM, Objekt 218

### Beispiele

- Auswahl von Benutzerkennungen 27
- Auswahl von Ereignissen 28
- Minimierung der Anzahl protokollierter Ereignisse 29

### Benutzer 304

### Benutzerattribute 304

### Benutzergruppe 304

### Benutzergruppeneintrag 304

### Benutzergruppenkennung 304

### Benutzerkatalog 304

### Benutzerkennung 304

#### SYSAUDIT 15

#### SYSPRIV 14

### Benutzerkennungskatalog 304

### Benutzerkommando 305

### Benutzerorganisation 305

### Benutzerrechte 305

### Benutzerverwaltung 305

### Betrieb

#### offline 310

#### online 310

### Betriebsmittel 315

### Beweis sichern 305

### Beweissicherung 305

## C

### Catalog Identification (CATID) 309

### CATALOG, Objekt 220

### CHANGE-SAT-FILE (SAT-Kommando) 76

### Command Profile 309

### CONSLOG / SKP2, Objekt 221

### CONSLOG-Datei 305, 312

#### aufbereiten 33, 140

### CONSLOG-Ereignisse 18

### COOWNER PROTECTION, Objekt 222

## D

### Data Protection 306

### Data Security 306

### DATA SPACES, Objekt 223

### Datei

#### Aufbereitung 33, 140

#### Eingabedatei SATUT 158

#### Katalog 305

#### SATUT 33, 140

### Daten

#### protokollieren 14

### Datensatz

#### ausdrucken 167

#### ausgeben 156

#### auswählen 156

#### drucken 140

#### sichern 140

#### sortieren 167

Datenschutz 306  
Datensicherung 306  
Datensichtstation 306  
DEFAULT PROTECTION, Objekt 224  
definieren  
    Rollen 312

## E

einfache Zugriffskrollliste 307  
Eingabedatei festlegen 158  
Ereignis  
    Beispiele 16  
    EVENT 16  
    Kurzname 196  
    permanent 17  
    protokollierbar 13  
    SAT 211  
EVENT 16, 22  
    Ereignis 16  
EVENTING-ITEM, Objekt 225

## F

Fachwörter 303  
Feldnamen  
    alphabetische Ordnung 213, 279  
    Werte 279  
    zugehörige Objekte 279  
File Directory (TSOSCAT) 305  
FILE, Objekt 226  
FILES-BY-EVENTS  
    Verknüpfungsbedingung 25  
Filter 307  
    aktivieren 31  
    ändern 93  
    Anwendungshinweis 73  
    anzeigen 127  
    definieren 68  
    löschen 117  
    MODIFY-SAT-FILTER-CONDITIONS 93  
    REMOVE-SAT-FILTER-CONDITIONS 117  
    SHOW-SAT-FILTER-CONDITIONS 127  
    speichern 122  
First-Start 307  
FITC, Objekt 228

Frist 307  
Function Accumulation 303  
Functionality Class 307  
Funktionalitätsklasse 307  
funktionelle Übersicht  
    SAT-Kommandos 56  
    SATUT-Anweisungen 146

## G

gemeinschaftlicher Speicherplatz 307  
Group Administrator 308  
Group Administrator Privilege 308  
Group Entry 304  
Group Identification 304  
Group Member 308  
GROUP, Objekt 229  
Gruppenkennung 307  
Gruppenmitglied 308  
Gruppenpotential 308  
Gruppenverwalter 308  
Gruppenverwalterrecht 308  
GUARDS  
    Objekt 230

## H

Hardware-Konfiguration, sichere 312  
HOLD-SAT-LOGGING (SAT-Kommando) 79

## I

Identifizierung 308  
Inbetriebnahme  
    SAT 54  
    SATUT 55  
INDEPENDENT-Logik  
    Bedingungen 24  
Installation 309  
    SAT 54  
    SATUT 55  
IPSEC, Objekt 231  
IT-Sicherheitskriterien 309

### J

JOB VARIABLES, Objekt 233  
JOB, Objekt 232  
Jobvariable, SAT-spezifisch 53  
Joinfile 304

### K

Katalogkennung (CATID) 309  
Kennwort 309  
Kommandoprofil 309

### M

Mehrrechnersysteme  
protokollieren 209  
MEMORY-POOL, Objekt 235  
MODIFY-SAT-ALARM-CONDITIONS (SAT-Kommando) 80  
MODIFY-SAT-FILTER-CONDITIONS (SAT-Kommando) 93  
MODIFY-SAT-PRESELECTION (SAT-Kommando) 106  
MODIFY-SAT-SUPPORT-PARAMETERS (SAT-Kommando) 113

### O

Objekt 310  
Definition 16  
Objekt ereignis  
protokollieren 279  
Objekt ereignisse  
Kurznamen 196  
Objekt ADAM 216  
Objekt ANY 216  
Objekt APPLICATION 217  
Objekt BCAM 218  
Objekt CATALOG 220  
Objekt CONSLOG / SKP2 221  
Objekt COOWNER PROTECTION 222  
Objekt DATA SPACES 223  
Objekt DEFAULT PROTECTION 224  
Objekt EVENTING-ITEM 225  
Objekt FILE 226  
Objekt FITC 228  
Objekt GROUP 229

Objekt GUARDS 230  
Objekt IPSEC 231  
Objekt JOB 232  
Objekt JOB VARIABLES 233  
Objekt MEMORY-POOL 235  
Objekt OPERATOR-ROLES 236  
Objekt PLAM-Elemente 237  
Objekt POSIX-CHILD-Process 239  
Objekt POSIX-FILE-and-Directory 240  
Objekt POSIX-PROCESS 247  
Objekt POSIX-SYSTEM-Resources 250  
Objekt PRIVILEGE 253  
Objekt PROGRAM 254  
Objekt SAT 256  
Objekt SAT-ALARM 259  
Objekt SAT-FILTER 260  
Objekt SESAM 261  
Objekt SMS 263  
Objekt SPOOL DEVICE 264  
Objekt SPOOL JOBS 265  
Objekt SUBSYSTEM 267  
Objekt SYNTAX FILE 268  
Objekt TAPE ENCRYPTION 269  
Objekt TERMINAL SET 271  
Objekt USERID 272  
Objekt UTM 274  
Objekt VOLUME 277  
Protokoll 213  
Standard-Protokollierung 196  
offline-Betrieb 310  
online-Betrieb 310  
Operator-Rolle 310  
OPERATOR-ROLES, Objekt 236

### P

Password 309  
Personal Audit for Individual Accountability 310  
personenbezogene Beweissicherung 310  
PLAM-Elemente, Objekt 237  
POSIX-CHILD-Process, Objekt 239  
POSIX-FILE-and-Directory, Objekt 240  
POSIX-PROCESS, Objekt 247  
POSIX-SYSTEM-Resources, Objekt 250  
Postselection 19, 33

- Preselection 19
  - Privileg 311
    - SAT 14
    - SAT-Datei-Auswertung 15
    - SAT-Datei-Verwaltung 15
    - SET-PRIVILEGE 303
    - Sicherheitsbeauftragter 14
  - PRIVILEGE, Objekt 253
  - Privilegienverwalter 310
  - Profil 311
  - PROGRAM, Objekt 254
  - Protokoll, Feldnamen 279
  - Protokolldatensatz
    - Analyse 33, 140
    - ausgeben 33, 140
    - Beispiel 52
    - fester Teil 50
    - globale Struktur 50
    - Header-Satz 49
    - Struktur 50
    - Trailer-Satz 49
    - variabler Teil 50
  - protokollierbares Ereignis 13
  - protokollieren
    - anhalten 79
    - beginnen 40
    - Daten 14
    - fortsetzen 118
    - Mehrrechnersysteme 209
    - Objekt ereignisse 196
    - SAT 40
    - System-Standard 21
    - Ziele 13
  - Public Space 307
  - Pubset 311
- Q**
- Qualitätsstufe 311
- R**
- Readme-Datei 9
  - Rechte
    - systemglobale 315
  - REMOVE-SAT-ALARM-CONDITIONS (SAT-Kommando) 116
  - REMOVE-SAT-FILTER-CONDITIONS (SAT-Kommando) 117
  - REMOVE-SELECTION-CONDITIONS (SATUT-Anweisung) 155
  - replacement-file 142
    - Eingabedateien ersetzen 142
    - erstellen 46
    - löschen 156
    - Namenskonvention 142
    - SAVE-SELECTED-RECORDS 156
    - SHOW-REDUCTION-FILES-ORIGIN 164
    - Verwendungszweck 142
    - Zusatzinformationen 142
  - RESUME-SAT-LOGGING (SAT-Kommando) 118
  - Retention Period 312
  - Right, Access 316
  - Rollen
    - definieren 312
    - SAT 14
    - SAT-Datei-Auswerter 15
    - SAT-Datei-Verwalter 15
    - Sicherheitsbeauftragter 14
- S**
- SAT 13
  - ADD-SAT-ALARM-CONDITIONS 60
  - ADD-SAT-FILTER-CONDITIONS 68
  - Auswahl-Regeln 24
  - Auswertung festlegen 213
  - Bedingungen festlegen 19
  - beenden 40
  - CHANGE-SAT-FILE 76
  - Dateien 54
  - Dateien, benötigte 54
  - Ereignis 211
  - Feldnamen auswählen 213
  - funktionelle Übersicht 56
  - HOLD-SAT-LOGGING 79
  - Information 124, 127, 131
  - Initialisierungswerte 22, 23
  - Installation 54

### SAT (Forts.)

- Kommandos 56
  - MODIFY-SAT-ALARM-CONDITIONS 80
  - MODIFY-SAT-FILTER-CONDITIONS 93
  - MODIFY-SAT-PRESELECTION 106
  - Objekt 256
  - Parameter-Datei 38, 41
  - Protokoll 211
  - protokollieren 40
  - REMOVE-SAT-ALARM-CONDITIONS 116
  - REMOVE-SAT-FILTER-CONDITIONS 117
  - RESUME-SAT-LOGGING 118
  - SHOW-SAT-ALARM-CONDITIONS 124
  - SHOW-SAT-FILTER-CONDITIONS 127
  - SHOW-SAT-STATUS 131
  - START-SATUT 144
  - starten 40
  - STARTUP 22, 23
  - Subsystem 54
  - Verknüpfungsregel 21
  - Zustand 131
- SAT anhalten 40
- SAT-Alarm, Einträge lesen 124
- SAT-ALARM, Objekt 259
- SAT-Datei
- Analyse 143
  - anlegen 46
  - Archivierung 142
  - auswählen 158
  - periodisch wechseln 46
  - wechseln 46, 57, 76
- SAT-Datei-Auswertung, Privileg 15
- SAT-Datei-Verwalter 15
- SAT-Datei-Verwaltung
- Aufgaben 15
  - Privileg 15
- SAT-Filter, Einträge lesen 127
- SAT-FILTER, Objekt 260
- SAT-Parameter sichern 38
- SAT-Parameter-Datei
- Alarm 41
  - ALARM-CONDITIONS 41
  - Erläuterungen 41
  - EVENT-PRESELECTION 41
  - explizit speichern 41
  - Fehler beim Öffnen 41
  - Filter 41
  - Name 41
  - SAT-FILE-ATTRIBUTES 41
  - Typ 41
  - Versionsumstieg 42
- SAT-Protokolldatei, siehe SATLOG-Datei
- SAT-Protokollierung
- Speicherplatzbedarf 47
  - Speichersättigung 48
- SAT-spezifische Jobvariable 53
- SATCP 40
- deaktivieren 40
  - SHUTDOWN 40
- SATLOG-Datei
- archivieren 46
  - aufbereiten 33
  - auswerten 33, 140
  - Auswertung 33, 45
  - Definition 50
  - DVS-Fehler 40
  - eröffnen 76, 118
  - implizit wechseln 46
  - Inhalt 50
  - löschen 46, 156
  - Namenskonvention 45
  - periodisch wechseln 46
  - protokollieren 50
  - schließen 76, 79
  - Schutz 45
  - speichern 46
  - überprüfen 40
  - verifizieren 40
  - wechseln 46
- SATUT
- Anweisungen 146
  - Arbeitsdateien 141
  - Ausgabe 141
  - Ausgabefunktion 140
  - ausgelieferte Dateien 55
  - Auswahlbedingungen festlegen 140
  - Auswertung 158
  - beenden 144

- SATUT (Forts.)
  - Dateitypen [142](#)
  - Eingabedatei [33](#), [140](#)
  - Eingabedateien [140](#), [141](#)
  - funktionelle Übersicht [146](#)
  - Grundfunktionen [140](#)
  - Inbetriebnahme [55](#)
  - Installation [55](#)
  - SATLOG-Datei auswerten [33](#), [140](#)
  - SAVE-SELECTED-RECORDS [156](#)
  - Schema einer Auswertung [140](#)
  - SELECT-INPUT-FILES [158](#)
  - SELECT-RECORDS [163](#)
  - Selektion durchführen [140](#)
  - SHOW-REDUCTION-FILES-ORIGIN [164](#)
  - SHOW-SELECTED-RECORDS [167](#)
  - starten [144](#)
  - Verwendung [33](#), [140](#)
  - Voraussetzungen [55](#)
- SAVE-SAT-PARAMETERS (SAT-Kommando) [120](#)
- SAVE-SELECTED-RECORDS (SATUT-Anweisung) [156](#)
- Schutzattribute [312](#)
- Schutzfrist [312](#)
- Security Administrator [313](#)
- Security Attributes [312](#)
- Security Audit Trail [13](#)
- Security Criteria [313](#)
- SECURITY-ADMINISTRATION
  - Privileg [14](#)
- SELECT-INPUT-FILES (SATUT-Anweisung) [158](#)
- SELECT-RECORDS (SATUT-Anweisung) [163](#)
- SESAM, Objekt [261](#)
- Session [315](#)
- SF-Pubset
  - siehe Pubset [311](#)
- SHOW-REDUCTION-FILES-ORIGIN (SATUT-Anweisung) [164](#)
- SHOW-SAT-ALARM-CONDITIONS (SAT-Kommando) [124](#)
- SHOW-SAT-FILTER-CONDITIONS (SAT-Kommando) [127](#)
- SHOW-SAT-STATUS (SAT-Kommando) [131](#)
- SHOW-SAT-SUPPORT-PARAMETERS (SAT-Kommando) [138](#)
- SHOW-SELECTED-RECORDS (SATUT-Anweisung) [167](#)
- SHOW-SELECTION-CONDITIONS (SATUT-Anweisung) [173](#)
- SHOW-STATISTICS (SATUT-Anweisung) [174](#)
- SHUTDOWN [312](#)
  - SATCP [40](#)
- Sichere Hardware-Konfiguration [312](#)
- Sicheres BS2000 [313](#)
- Sicherheitsbeauftragter [14](#), [21](#), [313](#)
  - SAT anhalten [40](#)
- Sicherheitskriterien [313](#)
- Sicherheitsverwalter [313](#)
- Single-Feature-Pubset
  - siehe Pubset [311](#)
- SKP2-Datei
  - aufbereiten [33](#), [140](#)
- SM-Pubset
  - siehe Pubset [311](#)
- SMS [314](#)
- SMS, Objekt [263](#)
- Sortierkriterium [167](#)
- Speicherplatz
  - gemeinschaftlicher [307](#)
- Speicherplatzbedarf, SAT-Datei [47](#)
- Speichersättigung, SAT [48](#)
- SPOOL DEVICE, Objekt [264](#)
- SPOOL JOBS, Objekt [265](#)
- SRPM [314](#)
- Standardeinstellung
  - für die Protokollierung [196](#)
- Standardwerte protokollieren [196](#)
- START-SATUT (SAT-Kommando) [144](#)
- START-SELECTION (SATUT-Anweisung) [186](#)
- STARTUP [314](#)
- Steuerfunktionen [19](#)
- Subjekt [314](#)
  - Definition [16](#)
  - USER [16](#)

### Subsystem

- Laden überwachen [32](#)
- SATCP [40](#)
- SUBSYSTEM, Objekt [267](#)
- Subsystemzugriff protokollieren [212](#)
- SYNTAX FILE, Objekt [268](#)
- SYSAUDIT, Benutzerkennung [15](#)
- SYSPRIV
  - Benutzerkennung [14](#)
- System Administration [315](#)
- System Resource [315](#)
- System-Exit
  - Ablaufschema (SAT) [32](#)
  - aktivieren [106](#)
  - Nr.110 [32](#)
- System-Managed-Pubset
  - siehe Pubset [311](#)
- Systemeinleitung [314](#)
- systemglobal
  - Rechte [315](#)
- systemglobale Benutzerverwaltung [314](#)
- Systemlauf [315](#)
- Systemressourcen [315](#)
- Systemverwalterrechte [315](#)
- Systemverwaltung [315](#)

### T

- TAPE ENCRYPTION, Objekt [269](#)
- Terminal [306](#)
- TERMINAL SET, Objekt [271](#)
- Terminal-Set [315](#)
- Typ, Zugriff [316](#)
- Type, Access [316](#)

### U

- Überlappungen vermeiden [161](#)
- USER [16, 21](#)
- User Administration [305, 314](#)
- User Attribute [304](#)
- User Command [305](#)
- User Group [304](#)
- User Identification (USER-ID) [304](#)
- User Privilege [305](#)
- USERID, Objekt [272](#)
- UTM-Ereignisse
  - protokollieren [37](#)
  - Subcode [212](#)
- UTM, Objekt [274](#)

### V

- Verknüpfungsregel (SAT) [21](#)
- VOLUME, Objekt [277](#)

### W

- Wahrheitstafeln [154](#)

### Z

- Zugang
  - Klasse [315](#)
- Zugangsschutz [316](#)
- Zugriff
  - protokollieren [45](#)
  - Typ [316](#)
- Zugriffsberechtigter [316](#)
- Zugriffsberechtigung (Access Admission) [316](#)
- Zugriffskontrollliste
  - einfache, Basic Access Control List (BACL) [307](#)
- Zugriffsrecht [316](#)
- Zugriffsschutz [316](#)