Fujitsu Technology Solutions

SECOS (BS2000/OSD)
Version V5.4A
Dezember 2012

Readme-Datei

1 Einleitung

Die vorliegende Readme-Datei zu SECOS V5.4 enthält Änderungen zu den folgenden Handbüchern:

[1] SECOS V5.3
Security Control System - Zugangs- und Zugriffskontrolle
Ausgabe Juli 2010
Bestellnummer: U5605-J-Z125-9

[2] SECOS V5.3
Security Control System - Beweissicherung
Ausgabe Juli 2010
Bestellnummer: U41845-J-Z125-1

2 Erhöhung der Anzahl an Eingabedateien beim Dienstprogramm SATUT

Bei der Anweisung SELECT-INPUT-FILES des Dienstprogramms SATUT wurde die Anzahl der Eingabedateien, die beim Operanden INPUT-FILES angegeben werden können, von 25 auf 100 heraufgesetzt.

Siehe hierzu Kap. 2.6.6, Anweisung SELECT-INPUT-FILES
auf Seite 157ff. im Handbuch [2].

```
SELECT-INPUT-FILES

INPUT-FILES = *STD(...) / list-poss(100): <filename 1..54>

      *STD(...)
         |
         |
           ...
```

INPUT-FILES =
Bestimmt die Dateitypen, die als Eingabe für die Aufbereitung dienen.

. . .

INPUT-FILES = list-poss(100): <filename 1..54>
Dateiname der analysis-file, die als Eingabe für SATUT dient.

3 Unterstützung weiterer Benutzerattribute in den Benutzergruppen

Die Kommandos ADD-USER-GROUP und MODIFY-USER-GROUP unterstützen einen neuen Klasse-2-Systemparameter und weitere 4 Benutzerattribute:

Siehe hierzu Kap. 3.4, Kommandos ADD-USER-GROUP auf Seite 149ff. und MODIFY-USER-GROUP auf Seite 254ff. im Handbuch [1].

```
ADD-USER-GROUP

...
,ADDRESS-SPACE-LIMIT = *STD / <integer 1..2147483647>
...
,HARDWARE-AUDIT = *ALLOWED / *NOT-ALLOWED
,LINKAGE-AUDIT = *ALLOWED / *NOT-ALLOWED
,CRYPTO-SESSION-LIMIT = *STD / *MAXIMUM /
                        <integer 0..32767>
,NET-STORAGE-USAGE = *ALLOWED / *NOT-ALLOWED
...
```

```
MODIFY-USER-GROUP

...
,ADDRESS-SPACE-LIMIT = *UNCHANGED / *STD /
                       <integer 1.. 2147483647>
...
,HARDWARE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
,LINKAGE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
,CRYPTO-SESSION-LIMIT = *UNCHANGED / *STD / *MAXIMUM /
                        <integer 0..32767>
,NET-STORAGE-USAGE = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
...
```

ADDRESS-SPACE-LIMIT = *STD
Der Standardwert wird im Startup-Parameterservice über den Klasse-2-Systemparameter SYSGJASL festgelegt. Er ist standardmäßig auf 16 MByte eingestellt.

HARDWARE-AUDIT = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, den Sprungfolgemodus (Hardware-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

LINKAGE-AUDIT = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, die Unterprogrammverfolgung (Linkage-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

CRYPTO-SESSION-LIMIT = *STD / *MAXIMUM / <integer 0..32767>
Vereinbart die maximale Anzahl openCRYPT-Sessions innerhalb einer BS2000[1]-Session, die vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

NET-STORAGE-USAGE = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, Speicherplatz auf einem Net-Storage Volume zu belegen, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

Das Kommando SHOW-USER-GROUP unterstützt die 4 Benutzerattribute:

– bei der Show-Ausgabe:

```
...
HARDWARE-AUDIT     ......   CRYPTO-SESSION-LIMIT     ......
LINKAGE-AUDIT      ......   NET-STORAGE-USAGE        ......
...
```

– durch Erzeugen von S-Variablen:

Name der S-Variablen	T	Inhalt
var(*LIST).HARDWARE-AUDIT	S	'*ALLOW' '*NOT-ALLOW'
var(*LIST).LINKAGE-AUDIT	S	'*ALLOW' '*NOT-ALLOW'
var(*LIST).CRYPTO-SESSION-LIM	I	<integer 0..32767>
var(*LIST).NET-STOR-USAGE	S	'*ALLOW' '*NOT-ALLOW'

Siehe hierzu Kap. 3.4, Kommando SHOW-USER-GROUP auf Seite 444ff. im Handbuch [1].

[1] BS2000/OSD® ist eine Marke von Fujitsu Technology Solutions.

4 Erweiterung der Ausgabe beim Kommando SHOW-LOGON-PROTECTION

Siehe hierzu Kap. 3.4, Kommando SHOW-LOGON-PROTECTION auf Seite 335ff. im Handbuch [1].

```
SHOW-LOGON-PROTECTION

. . .
,INFORMATION = *ATTRIBUTES(...) / ...

   *ATTRIBUTES(...)
      |    SCOPE = *LOGON-DEFAULT / *USER-IDENTIFICATION /
      |            *ALL
...
```

SCOPE = *ALL

Die Ausgabe zeigt neben den Attributen, die explizit für die Benutzerkennung festgelegt wurden, die aktuellen Standard-Attribute für die Zugangskontrolle, soweit sie für die Benutzerkennung gelten. Diese werden durch einen '*' gekennzeichnet.

Neue S-Variablen:

Siehe hierzu Seite 344ff. im Handbuch [1].

Name der S-Variablen	T	Inhalt
var(*LIST).EXPIR-DATE-DEF	B	FALSE TRUE
var(*LIST).EXPIR-WARN-DEF	B	FALSE TRUE
var(*LIST).PASS.MANAGE-DEF	B	FALSE TRUE
var(*LIST).PASS.MIN-LEN-DEF	B	FALSE TRUE
var(*LIST).PASS.MIN-COMPLEX-DEF	B	FALSE TRUE
var(*LIST).PASS.LIFETIME-DEF	B	FALSE TRUE
var(*LIST).PASS.EXPIR-DATE-DEF	B	FALSE TRUE
var(*LIST).PASS.EXPIR-WARN-DEF	B	FALSE TRUE
var(*LIST).PASS.UNLOCK-EXPIR-DEF	B	FALSE TRUE
var(*LIST).PASS.PASS-MEMORY-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.PAR-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.COUNT-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.OBS-TIME-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.SUS-TIME-DEF	B	FALSE TRUE
var(*LIST).SUSPEND.SUBJECT-DEF	B	FALSE TRUE
var(*LIST).INACTIVITY.PAR-DEF	B	FALSE TRUE
var(*LIST).DIALOG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).BATCH.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-TER.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-PROG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).OPER-CONS.ACCESS-DEF	B	FALSE TRUE
var(*LIST).POSIX-RLOG.ACCESS-DEF	B	FALSE TRUE
var(*LIST).POSIX-REM.ACCESS-DEF	B	FALSE TRUE
var(*LIST).NET-DIALOG.ACCESS-DEF	B	FALSE TRUE

5 Erweiterung des Makros SRMSUG

Der Makro SRMSUG unterstützt die 4 Benutzerattribute:

```
          SRMSUG XPAND=INFO,VERSION=6,MF=D
SRMAUG   DSECT ,
...
SRMAIND1 DS    X          INDICATOR BYTE 1:
SRMANSTU EQU   X'01'         NET-STORAGE-USAGE
**                              S: ALLOWED
**                              R: NOT ALLOWED
...
SRMAADSL DS    F          ADDRESS SPACE LIMIT
SRMAREPA DS    F          RESIDENT PAGES
SRMACRSL DS    F          CRYPTO SESSION LIMIT
...
```

Siehe hierzu Kap. 3.5, Makro SRMSUG auf Seite 459ff. im Handbuch [1].

6 Dialog-Logon in NET-DIALOG, ausweichen auf DIALOG

Siehe hierzu Kap. 3.3.6 auf Seite 108ff. im Handbuch [1].

Durch folgende Option in der Subsysteminfodatei SYSSSI.SRPMOPT.054:

NET-DIALOG-REJECT-FALLBACK=Y

wird der Dialog-Logon in der Zugangsklasse DIALOG ausgeführt, wenn die Kerberos-Prüfung in der Zugangsklasse NET-DIALOG zu keinem Ergebnis geführt hat, weil

1) das Ticket nicht entschlüsselt werden konnte oder
2) der im Ticket enthaltene Principal keine Zugangsberechtigung hat.

7 Korrektur eines Beispiels bei Single Sign On

Kap. 3.3.6 Single Sign On mit Kerberos, auf Seite 115 im Handbuch [1].

Die Beispiele für das Kommando ADD-KEYTAB-ENTRY unter dem ersten Spiegelstrich

```
/ADD-KEYTAB-ENTRY *STD('host/hostname@NT-DNS-REALM-NAME' -
/  ,KEY    = *PASSWORD('password')
```

und

```
/ADD-KEYTAB-ENTRY *STD('host/d016ze04.mch.fts.net@FTS.NET' -
/  ,KEY    = *PASSWORD('liebereinbisschenlaenger')
```

werden ersetzt durch

```
/ADD-KEYTAB-ENTRY *STD, 'host/hostname@NT-DNS-REALM-NAME' -
/  ,KEY    = *PASSWORD('password')
```

und

```
/ADD-KEYTAB-ENTRY *STD, 'host/d016ze04.mch.fts.net@FTS.NET' -
/  ,KEY    = *PASSWORD('liebereinbisschenlaenger',KEY-VERSION=3)
```

8 Korrektur bei CONVERT-KEYTAB

Kap. 3.4 SRPM-Kommandos, auf Seite 166 im Handbuch [1].

Bei "Einsatzvoraussetzungen" wird der Text

Hierzu muss
– die SRPMOPT-Option (Datei: SYSSSI.SRPMOPT.053) SECURITY-ADMIN-STD-PROCESSING=Y gesetzt werden, oder
– der Sicherheitsbeauftragte sich selber das Privileg STD-PROCESSING zuweisen.

ersetzt durch

Hierzu muss
– die SRPMOPT-Option (Datei: SYSSSI.SRPMOPT.054) SECURITY-ADMIN-STD-PROCESSING=Y gesetzt werden, **und**
– der Sicherheitsbeauftragte sich selber das Privileg STD-PROCESSING zuweisen.