

Effektive Crashdump-Analyse

DECUS IT-Symposium
VMS 1G06

Volker.Halle@invenate.de
05-APR-2005

Effektive Crashdump-Analyse

Was ist ein System-Crash ?

- ▶ Ursachen für System-Crashes
- ▶ System-Crash: System-Parameter und Dumpfile
- ▶ Was kommt nach dem Crash ?
- ▶ Do you have any CLUE ?
- ▶ Crash-Call Logging
- ▶ Crash-Analyse mit CCAT
- ▶ Analyse von SYSDUMP.DMP

Was ist ein System-Crash ?

▶ Zitate:

- „spontaner Neustart“
- „plötzlich sind alle User rausgeflogen“
- „der Bildschirm wurde plötzlich blau“
- „gestern war die System Uptime noch 90 Tage“

Was ist ein System-Crash ...

- ▶ OpenVMS erkennt Inkonsistenzen im Betriebssystem
 - Unexpected Exception
 - Zugriff auf ungültige virtuelle Adressen
 - Internal Data Structure Corruption
 - Überprüfung von internen Datenstrukturen
- ▶ Bei Inkonsistenzen im KERNEL des Betriebs-Systems wird ein Bugcheck erzeugt:
 - System Crash

Was ist ein System-Crash ... ?

- ▶ Bugcheck-Information wird auf Console Terminal ausgegeben
- ▶ System Memory wird auf Platte geschrieben (SYSTEM DUMP)
- ▶ System startet automatisch neu (REBOOT)

Was ist KEIN System-Crash ?

- ▶ System HALT >>>
 - HALT instruction im Kernel Mode
 - Kernel Stack not valid HALT
 - >>> SET AUTO_ACTION RESTART
- ▶ System Soft(ware) Hang
 - Control-P oder HALT-Knopf
 - >>> CRASH
- ▶ System Hard(ware) Hang
 - keine Reaktion auf HALT oder RESTART-Knopf

Warum ein System-Crash ?

- ▶ Zum Schutz der Anwender-Daten !
- ▶ Wiederherstellung der Konsistenz im Betriebs-System (durch Crash und Reboot)
- ▶ Dokumentation des System-Zustands für Fehleranalyse

Ursachen für System-Crashes

- ▶ Datenstruktur-Inkonsistenzen im Betriebs-System durch Coding Errors im Betriebs-System oder in privilegierten (CMKRNL) Programmen/Drivern
- ▶ Hardware/Firmware Fehler (selten !)
- ▶ Fehlbedienung durch privilegierte Benutzer (sehr selten !!)

Voraussetzungen für System-Dumps

- ▶ System Parameter
 - steuern das Verhalten bei einem System Bugcheck
- ▶ System Dump File
 - notwendig zum Abspeichern des System Memory bei einem System Crash

System-Crash - System-Parameter

- ▶ DUMPBUG = 1
 - =1 Dumpfile wird geschrieben (default)
 - =0 kein Dumpfile schreiben
 - ▶ SAVEDUMP = 0 (bei Dump in PAGEFILE.SYS)
 - =0 Pagefile-Space automatisch freigeben
 - =1 Dump im Pagefile nicht automatisch freigeben
- ```
$ ANAL/CRASH SYS$SYSTEM:PAGEFILE.SYS
SDA> COPY dir:[dev]crash.dmp
$ ANAL/CRASH/RELEASE SYS$SYSTEM:PAGEFILE.SYS
```

## System-Crash - System-Parameter...

▶ **DUMPSTYLE = 9**

Bit 0: 0 = Full Dump, 1 = Selective

Bit 1: 0 = Minimal Console Output, 1 = Full Output

Bit 2: 0 = Dump auf System-Disk, 1 = DOSD

Bit 3: 0 = no compression, 1 = Compressed dump

▶ **DUMPFILER=n (in MODPARAMS.DAT)**

= 0 AUTOGEN Dumpfile-Sizing ausschalten

= n Grösse des Dumpfiles in Blocks

## System-Crash - System-Parameter...

▶ **BUGCHECKFATAL = 0**

= 0 kein Crash bei non-fatal Bugcheck

Es wird nur ein Errlog-Entry (non-fatal bugcheck) erzeugt (meist EXEC-Mode, z.B. RMS).

= 1 System-Crash bei non-fatal Bugcheck

\$ MC SYSGEN

SYSGEN> USE ACTIVE

SYSGEN> SET BUGCHECKFATAL 1

SYSGEN> WRITE ACTIVE

## System-Crash - System-Parameter...

▶ **BUGREBOOT = 1**

0 = kein automatischer Reboot nach Crash

1 = automatischer Reboot nach System Crash

## System-Crash - Dumpfile

- ▶ System Dumpfile wird beim Booten gemapped  
Ausnahme: DOSD unter OpenVMS Alpha
- ▶ NIEMALS löschen
- ▶ Grösse ändern mit:  
SYSGEN> CREATE file/SIZE=n oder @AUTOGEN  
Reboot und evtl. PURGE
- ▶ entfernen mit:  
\$ RENAME SYSDUMP.DMP SYSDUMP.OLD  
Reboot  
\$ DELETE SYSDUMP.OLD;

## System-Crash - Dumpfile...

- ▶ **SYS\$SYSTEM:SYSDUMP.DMP**  
muss in SYS\$SPECIFIC:[SYSEXE] existieren
- ▶ **SYS\$SYSTEM:PAGEFILE.SYS**  
wenn kein SYSDUMP.DMP vorhanden  
SAVEDUMP=1 setzen  
beim Startup: SDA> COPY/COMPRESS  
dev:[dir]file.dmp

## System-Crash - Dumpfile...

- ▶ **COMMON\_SYSDUMP.DMP im Cluster**  
Berechnung der Grösse des Dumpfiles mit:  
@AUTOGEN GETDATA TESTFILES  
... A nnnnn block dump file would have been created  
  
SYSGEN> CREATE SYS\$COMMON:[SYSEXE]SYSDUMP-COMMON.DMP -  
/SIZE=nnnnn  
\$ SET FILE SYS\$COMMON:[SYSEXE]SYSDUMP-COMMON.DMP -  
/ENTER=SYS\$SYSDEVICE:[SYSn.SYSEXE]SYSDUMP.DMP  
  
DUMPFIL=0 in allen MODPARAMS.DAT, um Dumpfile Auto-Sizing  
durch AUTOGEN zu verhindern

## System-Crash - Dumpfile...

### ▶ DOSD Dump Off System Disk (OpenVMS Alpha)

disk:[SYSn.SYSEXE]SYSDUMP.DMP

DUMPSTYLE - Set Bit 2

Mount DOSD Disk in SYLOGICALS.COM:

MOUNT/SYS/NOASSIST disk label CLUE\$DOSD\_DEVICE

oder

DEFINE/SYSTEM CLUE\$DOSD\_DEVICE disk

>>> SET DUMP\_DEV DKAx

MODPARAMS.DAT: DUMPFILe\_DEVICE="\$n\$DKAx:"

## DUMP\_DEV Console Variable

▶ alle möglichen Pfade zur System/Dump-Disk eintragen

▶ max. 4 Einträge möglich

▶ zuerst DOSD-Disk (falls vorhanden), dann System-Disk (wegen SYS\$ERRLOG.DMP)

>>> SET DUMP\_DEV DGA0.1001,DGA0.1002,DGB0.1003,DGB0.1004

## Was kommt nach dem Crash ?

- ▶ Automatischer Reboot (BUGREBOOT=1)
- ▶ Automatische Erzeugung des Crash-Footprints

OpenVMS Alpha:

CLUE\$COLLECT:CLUE\$node\_ddmmy\_hhmm.LIS

OpenVMS VAX:

CLUE\$OUTPUT:CLUE\$LAST\_node.LIS

- ▶ Crash-Analyse

Analyse auf Basis des CLUE-Files

Crash-Analyse mit SDA

## Do you have any CLUE ?

- ▶ CLUE = Crash Log Utility Extractor
  - erzeugt automatisch Crash Footprint File aus dem System Dump File
  - wichtigste Informationen über den System Crash
  - Datei in Text-Format
    - klein (50.-100. Blocks)
    - lesbar
    - per e-mail leicht zu versenden

## Do you have any CLUE... ?

### ► Implementation

OpenVMS Alpha seit V6.1

SDA Extension: SYS\$SHARE:CLUE\$SDA.EXE

SDA> CLUE HELP

OpenVMS VAX seit V6.0

SYS\$SYSTEM:CLUE.EXE

\$ CLUE:==\$CLUE

\$ CLUE HELP

## Do you have any CLUE... ?

### ► OpenVMS Alpha

Crash Historie (letzte 50 Crashes im Cluster)

\$ TYPE CLUE\$HISTORY ! 132 columns

| Date              | Version | System/CPU       | Node | Bugcheck   | Process  | PC       | Module               | Offset   |
|-------------------|---------|------------------|------|------------|----------|----------|----------------------|----------|
| 14-JUL-1999 18:09 | V7.1    | DEC 3000 - M300X | HAN  | INVEXCEPTN | HALLE    | 8018E210 | SYSSNETWORK_SERVICES | 00006210 |
| 15-JUL-1999 13:44 | V7.1    | DEC 3000 - M300X | HAN  | INVEXCEPTN | FISCHER  | 8018E210 | SYSSNETWORK_SERVICES | 00006210 |
| 09-SEP-1999 09:29 | V7.1    | DEC 3000 - M300X | HAN  | INCONSTATE | NULL     | 8022CB7C | SYSSPKCDRIVER        | 00008B7C |
| 13-DEC-1999 12:35 | V7.1    | DEC 3000 - M300X | HAN  | OPERATOR   | _TNA148: | 0003060C | OPCCRASH             | 0003060C |
| 21-SEP-2000 10:33 | V7.1    | DEC 3000 - M300X | HAN  | OPERCRAASH | NULL     | 8009B220 | PROCESS_MANAGEMENT   | 00001220 |
| 10-NOV-2000 11:13 | V7.1    | DEC 3000 - M300X | HAN  | OPERCRAASH | NULL     | 8009B164 | PROCESS_MANAGEMENT   | 00001164 |

## Do you have any CLUE... ?

### ▶ OpenVMS Alpha

Footprints der letzten Crashes:

```
$ DIR CLUE$COLLECT:CLUE$node*.LIS
```

```
$ TYPE CLUE$COLLECT:CLUE$node_ddmmyy_hhmm.LIS
```

### ▶ CLUE Troubleshooting:

CLUE File wird erzeugt im Prozess CLUE\$SDA beim Startup

Fehlermeldungen sind in:

```
$ TYPE SYS$MANAGER:CLUE$STARTUP.LOG
```

## Do you have any CLUE... ?

```
Crash Time: 9-SEP-1999 09:29:25.04
Bugcheck Type: INCONSTATE, Inconsistent I/O data base
Node: HAN (Standalone)
CPU Type: DEC 3000 - M300X
VMS Version: V7.1
Current Process: NULL
Current Image: <not available>
Failing PC: FFFFFFFF.8022CB7C SYS$PKCDRIVER_NPRO+08B7C
Failing PS: 18000000.00001504
Module: SYS$PKCDRIVER
Offset: 00008B7C

Boot Time: 7-SEP-1999 13:04:02.00
System Uptime: 1 20:25:23.04
```

## Do you have any CLUE... ?

### ► OpenVMS VAX

Crash Historie (letzte 100 Crashes & Shutdowns):

\$ CLUE/DISPLAY

| # | Node | Time             | Type     | Process Name | Module    | Offset |
|---|------|------------------|----------|--------------|-----------|--------|
| 1 | RF4  | 9-FEB-1998 00:12 | CLUEXIT  | NONE         | CLUSTRLOA | AF7    |
| 2 | RF4  | 8-FEB-1998 19:57 | CLUEXIT  | NONE         | CLUSTRLOA | AF7    |
| 3 | RF4  | 8-FEB-1998 19:46 | CLUEXIT  | NONE         | CLUSTRLOA | AF7    |
| 4 | RF4  | 7-FEB-1998 20:01 | OPERATOR | _OPA0:       | UNKNOWN   | 0      |

Problem mit CLUE\$OUTPUT:CLUE\$HISTORY.DATA (Illegal Format) unter OpenVMS VAX V7.2: Lösung verfügbar (Referenz: CFS.70650)

## Do you have any CLUE... ?

### ► OpenVMS VAX:

CLUE File des letzten Crashes:

\$ TYPE CLUE\$OUTPUT:CLUE\$LAST\_node.LIS

vorherige Crashes:

\$ CLUE/DISPLAY

CLUE> n ! zeigt CANASTA Parameter

CLUE> SHOW ALL n ! zeigt alle CLUE Daten

## Do you have any CLUE... ?

Canasta Parameters: (am Ende des OpenVMS VAX CLUE Files)

|                  |             |
|------------------|-------------|
| VMS Version      | : 7.1       |
| Crash Type       | : CLUEXIT   |
| Current Process  | : NONE      |
| Current Image    | : NONE      |
| CPU Type         | : 4000-60   |
| SID              | : 12000003  |
| Signal Array Cnt | : 0         |
| Exception par #1 | : FFFFFFFF  |
| Exception par #2 | : FFFFFFFF  |
| Exception par #3 | : FFFFFFFF  |
| Exception PC     | : 826BDAF7  |
| Exception PSL    | : 04080000  |
| Failing Inst     | : BUGW      |
| Code Module      | : CLUSTRLOA |
| Offset           | : AF7       |

## Do you have any CLUE... ?

- ▶ **OpenVMS Alpha CLUE Files**
  - wichtigstes Tool zur Früherkennung des Crashes
  - zusätzliche Informationen abhängig vom Bugcheck (z.B. bei CPUSPINWAIT Crash)
  - wird ständig weiterentwickelt und verfeinert (z.B. Dekodierung der Register-Inhalte)
  - gibt guten Überblick über Crash-Szenario

## Peeking at the dump ...

- ▶ ANA/CRASH von anderer Maschine (z.B. im Cluster) vor Reboot
- ▶ es wird kein CLUE File erzeugt beim STARTUP  
%CLUE-I-ALRDYANA, dumpfile has already been analyzed
- ▶ **WORAROUND:**  
\$ ANA/CRASH dumpfile  
SDA> READ/EXEC/NOLOG  
SDA> CLUE HISTORY/OVERRIDE

## Crash Call Logging

### Störungsmeldung nach System Crashes:

- ▶ **telefonisch**  
Bugcheck Type, VMS Version, Module+Offset  
CLUE-File per e-mail an CSC senden
- ▶ **elektronisch**  
über CCC
- ▶ **automatisch über PRS (DSNlink/ISEE)**  
mit CADC (AutoCLUE) oder WEBES/CCAT

## Crash Call Logging...

▶ Automatisches Crash-Call-Logging mit PRS/DSNlink

CADC = Crash Analysis Data Collector

vormals: AutoCLUE

Download von HP Service Tools

<http://h71025.www7.hp.com/support/tools/index.asp>

> WEBES

> CCAT

> CADC - aktuell V3.0

unterstuetzt PRS (Proactive Remote Services), DSNlink oder Mail

## Crash Call Logging...

▶ CADC V3.0

Installation mit

@VMSINSTAL CADC-OPENVMS

2 Logicals in SYLOGICALS.COM einfügen:

```
$ DEFINE/SYSTEM CADC$PROFILE -
 SYS$xxx:[CADC]CADC$PROFILE.DAT
```

```
$ DEFINE/SYSTEM CADC$OUTPUT -
 SYS$xxx:[CADC]
```

xxx = Installation in SYS\$SPECIFIC oder SYS\$COMMON

## Crash Call Logging...

### ▶ CADC...

Aufruf im Startup mit

@SYS\$STARTUP:CADC-OPENVMS

falls neues CLUE File existiert, wird Mail an System Manager und PRS/DSNlink gesendet (falls konfiguriert)

### ▶ Automatische Crash-Analyse findet bei HP statt (mit CCAT im Support-Center)

## Crash-Analyse mit CCAT

### ▶ CCAT = Computer Crash Analysis Tool

Bestandteil von WEBES (Web-Based Enterprise Services: CA, CCAT, RCM)

auf System Tools CD oder von HP Services

aktuell: WEBES V4.4 - ab OpenVMS Alpha V7.2-2

Installation mit @WEBES\_INSTALL

Do you want to install the Compaq Crash Analyze tool [YES]?

Einsatz alternativ zu CADC/AutoCLUE

## Crash-Analyse mit CCAT...

- ▶ Crash Knowledge Database (CCAT Rules) mit Lösungen von bekannten Crash-Problemen  
Troubleshooting Informationen
- ▶ Crash-Analyse mit CCAT auf lokalem System  
keine elektronische Verbindung (CPRS) zu HP  
notwendig  
CCAT analysiert CLUE Files  
Informationen von SDA> CLUE CRASH

## Crash-Analyse mit CCAT...

- ▶ Crash Knowledge Database (CCAT Rules V4.3)

OpenVMS Alpha:

1845 CCAT Rules insgesamt

OpenVMS VAX:

2102 CCAT Rules insgesamt

Kunde sieht nur CCAT-Rule-ID (z.B. CCAT-V-A-1234)

## Crash-Analyse mit CCAT...

- ▶ **Automatische Crash-Analyse beim Startup**
  - Mail an System Manager
  - automatischer Crash-Call ueber ISEE, PRS oder DSNlink
- ▶ **Manuelle Analyse von CLUE Files**
  - \$ @SVCTOOLS\_HOME:[COMMON.BIN]WCCAT GUI
  - JAVA-basierend. MOTIF User Interface.
  - Eigenes JRE (Java Runtime Environment) im CCAT Directory

## Analyse von SYSDUMP.DMP

- ▶ **Dump-Analyse mit SDA**
  - \$ ANA/CRASH SYS\$SYSTEM:SYSDUMP.DMP
  - SDA> HELP und CLUE HELP
  - SDA> CLUE CRASH
  - SDA> COPY/COMPRESS disk:<dir>file.dmp
- ▶ **BACKUP/IGNORE=NOBACKUP !!!**
  - SYSDUMP.DMP ist auf /NOBACKUP per Default
  - \$ DIR/FULL zeigt: Backups disabled

## Effektive Crashdump-Analyse

- ▶ System Dumpfile und System-Parameter korrekt konfigurieren
- ▶ >>> SET AUTO\_ACTION RESTART  
zum Aufzeichnen von Restart-Crashes  
WRITE SYS\$OUTPUT F\$GETENV("AUTO\_ACTION")
- ▶ ISEE/PRS/DSNlink und CCAT/CADC verwenden
- ▶ Informationen aus CLUE File verwenden bei Störungsmeldungen für Crashes