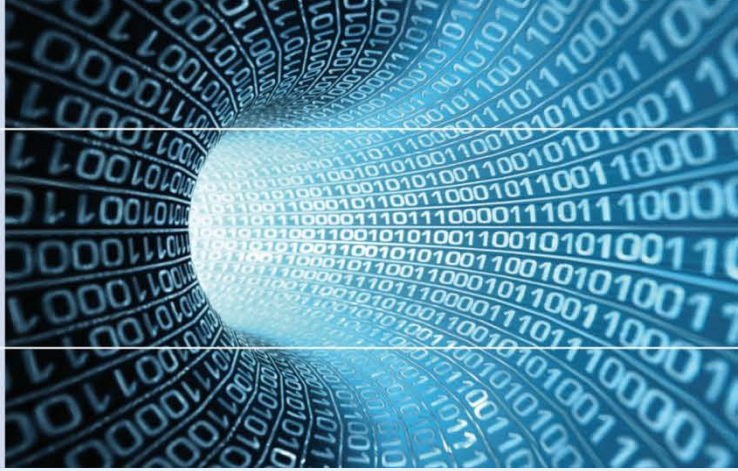
PDV SYSTEME
IHR PARTNER FÜR HOCHFORMANTE IT



The Secrets of EFI

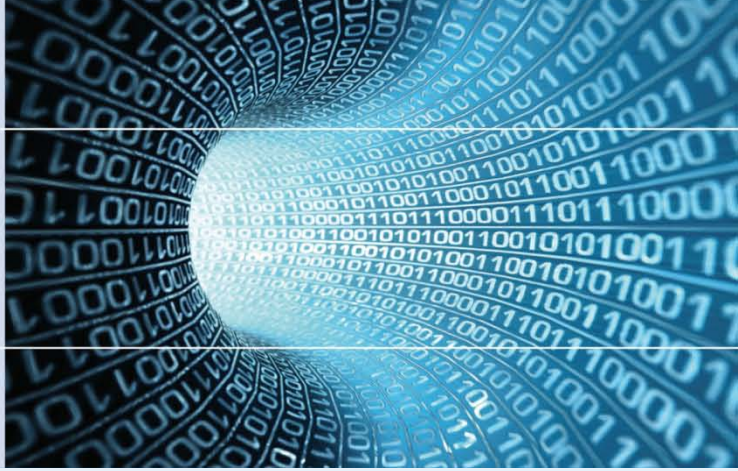
OpenVMS Technical Update Days 2012

Martin Vorländer

PDV-Systeme GmbH
Dörntener Straße 2A
D-38644 Goslar

PDV▸SYSTEME

IHR PARTNER FÜR HOCHFORMANTE IT



HP Integrity Servers and their Consoles

OpenVMS Technical Update Days 2012

Martin Vorländer

PDV-Systeme GmbH
Dörntener Straße 2A
D-38644 Goslar

Agenda

- Intel Itanium and HP Integrity Server
- Consoles of HP Integrity Servers
- The Management Processor
- The Extensible Firmware Interface (EFI)
- The EFI Shell
- Examples of EFI Commands

Agenda

- **Intel Itanium and HP Integrity Server**
- Consoles of HP Integrity Servers
- The Management Processor
- The Extensible Firmware Interface (EFI)
- The EFI Shell
- Examples of EFI Commands

Disambiguation: IA64 – Itanium – IPF – Integrity

IA64 → "Intel Architecture 64 Bit"

processor architecture and EPIC instruction set

Itanium → IA64 processor type by Intel

IPF → "Itanium Processor Family"

if not refering to a specific Itanium processor

Integrity → family of HP systems with an IPF processor

but: HP OpenVMS **I64**
→ "HP OpenVMS Industry Standard 64 for HP Integrity Servers"

Intel Itanium 2

Code name	released	CPU (GHz)	Cores	L3 Cache / Core (MB)	Family, Model	
Merced	2001	0.7 – 0.8	1	(4 extern)	7,0	Itanium 1
McKinley	2002	0.9 – 1.0	1	1.5 – 3	31,0	
Madison	2003 - 2004	1.3 – 1.6	1	1.5 – 6	31,1	
Deerfield	2003	1.0	1	1.5	31,1	LV Madison
Madison 9M	2004	1.6	1	9	31,2	
Fanwood	2004	1.3 – 1.6	1	3	31,2	LV Madison 9M
Montecito	2006	1.4 – 1.6	1 , 2	4 – 12	32,0	Series 90xx
Montvale	2007	1.42 – 1.66	1 , 2	4 – 12	32,1	Series 91xx
Tukwila	2010	1.33 – 1.73	2 , 4	4 – 6	32,2	Series 93xx
Poulson	*2012*	*?*	*8*	*(54 LLC)*	*?*	*Series 95xx*
Kittson	*2014?*	*?*	*?*	*?*	*?*	

HP Integrity Server

Workstation

i2000 zx2000 zx6000

Entry-level Server (2 CPU sockets)

rx1600 rx1620

rx2600 rx2620 **rx2660** **rx2800 i2**

rx3600

BL860c **BL860c i2**

Entry-level Server (4 CPU sockets)

rx4610 rx4640

rx5670

rx6600

BL870c **BL870c i2**

Mid-range Server (cell-based)

rx7620 **rx7640**

rx8620 **rx8640**

rx9610

BL890c i2

High-End Server (cell-based)

Superdome

Superdome 2

Color key:

Merced / McKinley

Madison

Montecito / Montvale

Tukwila

Agenda

- Intel Itanium and HP Integrity Server
- **Consoles of HP Integrity Servers**
- The Management Processor
- The Extensible Firmware Interface (EFI)
- The EFI Shell
- Examples of EFI Commands

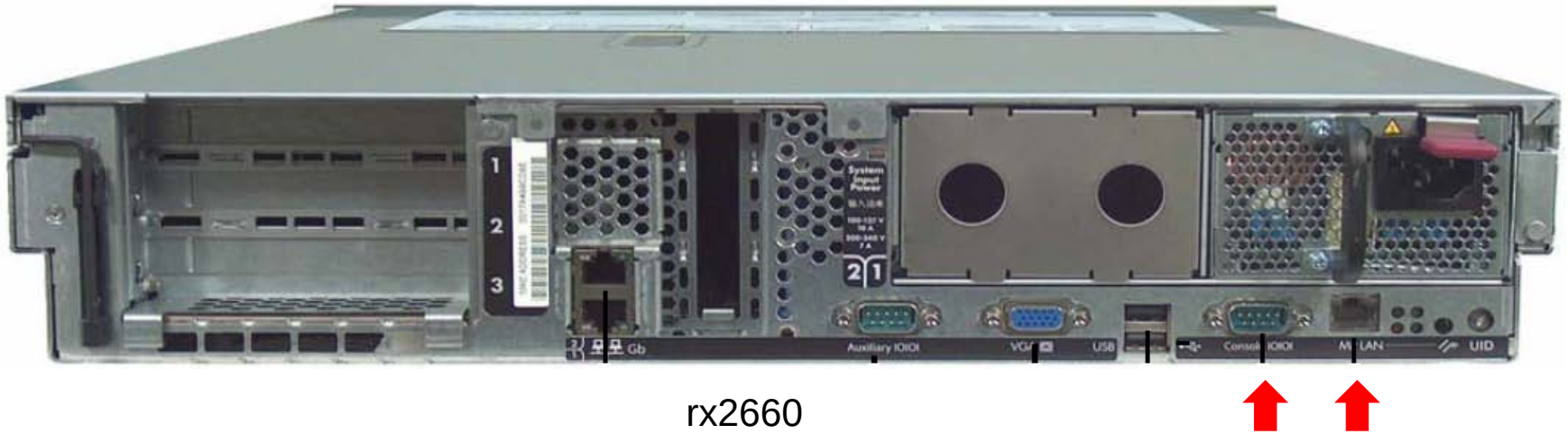
HP Integrity: Consoles

- **Baseboard Management Controller (BMC)**
  - works as soon as the mainboard is connected to power
  - connectivity: serial
  - self tests
  - device discovery
  - IPMI + HP extensions
- **Management Processor (MP)**
  - works as soon as the system is connected to power
  - connectivity: serial, modem, IPv4 (Telnet, SSH, Web)
  - manages access to the system console
    - concurrent mirrored sessions possible (with one writer)
  - (T)FTP (→ firmware updates)
  - user administration locally or via LDAP
  - iLO (integrated Lights-Out) management
- **System Console / EFI Shell**
  - works when the system is powered on

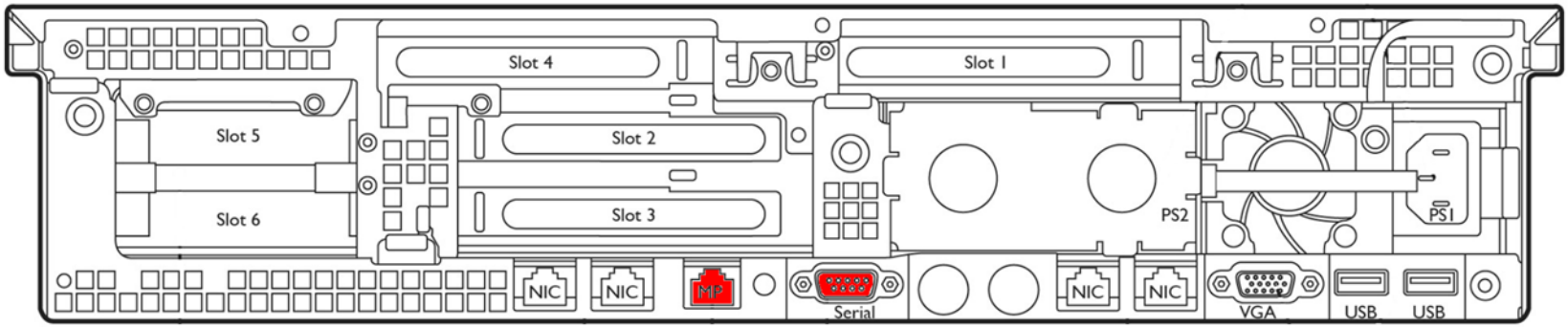
Agenda

- Intel Itanium and HP Integrity Server
- Consoles of HP Integrity Servers
- **The Management Processor**
- The Extensible Firmware Interface (EFI)
- The EFI Shell
- Examples of EFI Commands

Accessing MP



rx2660



rx2800 i2

PDV SYSTEME
hochformante IT®

Connecting to MP

- serial console port (9600 bps, 8N1)
  - If the system console is running: Ctrl+B
- MP LAN via Telnet or SSH

```
**********************************************************************
 This is a private system.
 Do not attempt to login unless you are an authorized user.
 Any authorized or unauthorized access or use may be monitored and can
 result in criminal or civil prosecution under applicable law.
**********************************************************************

**********************************************************************
 Only default users are configured.
 Use one of the following user/password pairs to login:

 Admin/Admin
 Oper/Oper
**********************************************************************

MP login:
```

MP: Main Menu

```
MP MAIN MENU:

        CO: Console
       VFP: Virtual Front Panel
        CM: Command Menu
        CL: Console Log
        SL: Show Event Logs
          …
        HE: Main Help Menu
         X: Exit Connection

[nodename] MP>
```

MP: Console

- `MP> CO`
  connects the MP session to the system console
- Switch from system console to MP: Ctrl+B
- If another console session is open already,
  upon entering the first character:
  `[Read only - use Ctrl-Ecf for console write access.]`
- Typing **Ctrl+E c f** results in:
  `[bumped user - otherUser]`
  and the session is granted write access
- In the other console session:
  `[returned to read only mode by user – myUser]`
  `[Read only - use Ctrl-Ecf for console write access.]`

MP: Command Menu

```
[nodename] MP> CM
[nodename] MP:CM> HE LI

==== MP Help: Command Menu List ============================================

BP   : Reset BMC Passwords              MS   : Modem Status
CA   : Configure asynch/serial ports    PC   : Remote Power Control
DATE: Display Date                      PG   : PaGing parameters setup
DC   : Default Configuration            PR   : Power Restore Policy Config.
DF   : Display FRU Information          PS   : Power management module Status
DI   : DIsconnect users                 RB   : Reset BMC
DNS  : Configure DHCP and DNS           RS   : Reset System through RST signal
FW   : Upgrade MP firmware              SA   : Set MP Access
HE   : Display Help                     SNMP: Configure SNMP parameters
ID   : System Information               SO   : Security Options
IT   : Modify MP inactivity timeouts    SS   : System processors Status
LC   : Configure LAN, SSH and Web ports SYSREV: Display System firmware Revs.
LDAP: Configure Directory parameters    TC   : Reset system via INIT
LM   : License Management               TE   : TEll- send a msg. to other users
LOC  : Locator LED display              UC   : User Configuration
LS   : LAN Status                       WHO  : Display connected MP users
MR   : Modem Reset                      XD   : Diagnostics and reset of MP
```

MP: Command PC – Power Control

```
[nodename] MP:CM> HE PC

==== MP Help: Server Control ================================================

  PC  : Power Control

Command access level: Power Control access.

PC command provides the following options for remote control of the system power:
"ON"    - turns system power on (it has no effect if power is already on).
"OFF"   - turns system power off.
          This command is roughly equivalent to turning the system power off
          with the front panel power switch- there is no signal sent to the OS
          to bring the software down before power is turned off.  For proper
          system shutdown, shutdown the OS before issuing this command.
"CYCLE" - turns system power off and on.  The delay between off and on
          is 30 seconds.
"GRACEFUL SHUTDOWN - BMC send a signal to the OS to shutdown prior to
          turning off system power

 SEE ALSO:  PR, PS  (Power Restore policy configuration, Power Status)


[nodename] MP:CM> PC

Current System Power State: On

Power Control Menu:
     C   - Power Cycle
     ON  - Power On
     OFF - Power Off
     G   - Graceful Shutdown

Enter menu item or [Q] to Quit: Q


[nodename] MP:CM> PC -OFF

System will be powered off.

   You must shut down the OS manually before this command is executed.
   Failure to do this can cause problems when the OS is restarted.
   Confirm? (Y/[N]): Y

 -> System is being powered off.

-> Command successful.
```

MP: Command LC – LAN Configuration

```
[nodename] MP:CM> HE LC

==== MP Help: Port Configuration ============================================

  LC  : LAN Configuration usage (IP address, etc.)

Command access level: MP Configuration access.

This command modifies the LAN Configuration.  Configurable parameters: DHCP
enable/disable, MP IP Address, MP host name, subnet mask, gateway, web
access port number, SSH access port number, LAN speed, and autonegotiation.
…
Command line usage:
  LC [ -ip <ipaddr> ] [ -subnet <subnet> ] [ -gateway <ipaddr> ]
     [ -host <hstname> ] [ -web <port> ] [ -link <auto|T(10baseT)> ]
     [ -ssh <port> ] [ -dhcp <e|d> ] [ -nc ]

SEE ALSO:  DNS, LS, SA  (DNS Configuration, LAN Status, Set Access)
```

MP: Event Logs

```
[nodename] MP> SL

Event Log Viewer Menu:
       Log Name             Entries    % Full      Latest Timestamped Entry
-------------------------------------------------------------------------------
   E - System Event           168        18 %      15 Apr 2011 09:45:52
   F - Forward Progress       828        20 %      15 Apr 2011 09:45:52
   B - Current Boot            77        25 %
   P - Previous Boot           77        25 %
   C - Clear All Logs
   L - Live Events

Enter menu item or [Ctrl-B] to Quit:
```

MP: System Event Log

```
Enter menu item or [Ctrl-B] to Quit: E

       Log Name            Entries    % Full      Latest Timestamped Entry
-------------------------------------------------------------------------------
   E - System Event          168        18 %      15 Apr 2011 09:45:52

Event Log Navigation Help:
   +       View next block     (forward in time,  e.g. from 3 to 4)
   -       View previous block (backward in time, e.g. from 3 to 2)
   <CR>    Continue to the next or previous block
   D       Dump the entire log
   F       First entry
   L       Last entry
   J       Jump to entry number
   H       View mode configuration - Hex
   K       View mode configuration - Keyword
   T       View mode configuration - Text
   A       Alert Level Filter options
   U       Alert Level Unfiltered
   ?       Display this Help menu
   Q       Quit and return to the Event Log Viewer Menu
   Ctrl-B  Exit command, and return to the MP Main Menu

MP:SL (+,-,<CR>,D, F, L, J, H, K, T, A, U, ? for Help, Q or Ctrl-B to Quit) >
```

MP: System Event Log (cont.)

```
MP:SL (+,-,<CR>,D, F, L, J, H, K, T, A, U, ? for Help, Q or Ctrl-B to Quit) > L

#  Location|Alert| Encoded Field    |  Data Field    |   Keyword / Timestamp
-------------------------------------------------------------------------------
167   OS   0   1  0x548016E100E00BF0 0000000000000001 OS_BOOT_COMPLETE
                                                      15 Apr 2011 09:45:52
166   BMC      2  0x204DA81324020BE0 FFFF0103FDC00300 Type-02 c00301 12583681
                                                      15 Apr 2011 09:43:00
165   BMC      2  0x204DA81321020BD0 FFFF0103FDC00300 Type-02 c00301 12583681
                                                      15 Apr 2011 09:42:57
164   SFW  0   1  0x5480020B00E00BB0 0000000000000006 EFI_LAUNCH_BOOT_MANAGER
                                                      15 Apr 2011 09:24:45
163   SFW      2  0xC14DA80EDD020BA0 FF8F416F00120300 Type-02 126f01 1208065
                                                      15 Apr 2011 09:24:45
162   BMC      2  0x204DA80EC3020B90 FFFF0103FDC00300 Type-02 c00301 12583681
                                                      15 Apr 2011 09:24:19
161   SFW  0   1  0x5680006300E00B70 0000000000000000 BOOT_START
                                                      15 Apr 2011 09:24:13
160   SFW      2  0xC14DA80EBD020B60 FFFF000A001D0300 Type-02 1d0a00 1903104
                                                      15 Apr 2011 09:24:13
159   BMC      2  0x204DA80EBD020B50 FFFF027000120300 Type-02 127002 1208322
                                                      15 Apr 2011 09:24:13
```

MP: System Event Log (cont.)

```
MP:SL (+,-,<CR>,D, F, L, J, H, K, T, A, U, ? for Help, Q or Ctrl-B to Quit) > T
MP:SL (+,-,<CR>,D, F, L, J, H, K, T, A, U, ? for Help, Q or Ctrl-B to Quit) > L

Log Entry 167: 15 Apr 2011 09:45:52
Alert Level 1: Major Forward Progress
Keyword: OS_BOOT_COMPLETE
OS Boot Complete
Logged by: O/S Kernel (Generic)  0
Data: Major change in system state - Boot Complete
0x548016E100E00BF0 0000000000000001

Log Entry 166: 15 Apr 2011 09:43:00
Alert Level 2: Informational
Keyword: Type-02 c00301 12583681
Time Set
Logged by: Baseboard Management Controller;
Sensor: SEL Time Set
Data1: State Asserted
0x204DA81324020BE0 FFFF0103FDC00300

MP:SL (+,-,<CR>,D, F, L, J, H, K, T, A, U, ? for Help, Q or Ctrl-B to Quit) >
```

Agenda

- Intel Itanium and HP Integrity Server
- Consoles of HP Integrity Servers
- The Management Processor
- **The Extensible Firmware Interface (EFI)**
- The EFI Shell
- Examples of EFI Commands

Extensible Firmware Interface (EFI)

- Specification of a software interface that sits between the platform firmware and the OS
- History
  - 1998: “Intel Boot Initiative“
  - developed by Intel
    for the first HP Itanium systems (among others)
    - PC-BIOS was regarded as inadequat
  - 2005: Unified EFI Forum
    - AMD, American Megatrends, Apple, Dell, HP, IBM, Insyde Software, Intel, Lenovo, Microsoft, Phoenix Technologies
    - EFI 1.10
    - Renamed to Unified EFI (UEFI)
- current version: 2.3.1C

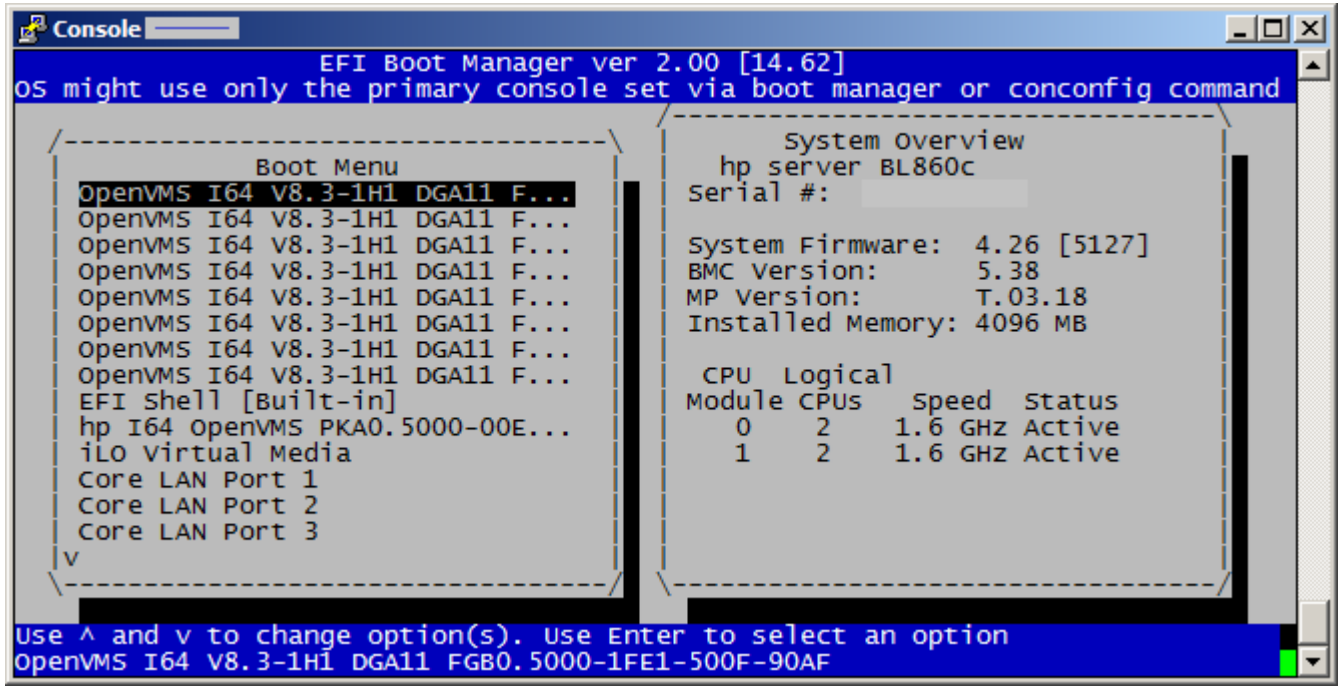
EFI: Characteristics

- platform and OS independant
- 32 and 64 bit
  - PC-BIOS: 16 bit, 1MB address space (original design for the Intel 8088)
- modular design
- EFI Byte Code (also for drivers!)
- new partitioning scheme for harddisks
  - GPT (GUID Partition Table)
  - max. disk/partition size: 9.4 Zettabyte (1 ZB = 1,000,000,000 TB)
    - PC-BIOS: MBR, max. disk/partition size 2.2 TB
- Boot Manager
  - primary OS bootloader is an EFI Application
- platform independant support for graphical output
- extensions:
  - shell
  - network support
  - support for ACPI and SMBIOS

EFI implementations

- HP
  - all HP Integrity Server
    - “POSSE“ (Pre-OS System Environment)
      - includes commands compatible with PA-RISC BCH
  - various HP Notebooks and Tablet PCs
- Apple: all Intel based Macs
  - graphical Boot Manager
  - no shell
    - SourceForge project rEFIt
- other PC mainboard manufacturers
- many mainboards with Sandy Bridge processor
- BIOS emulation CSM (Compatibility Support Module)

Examples of EFI Boot Managers

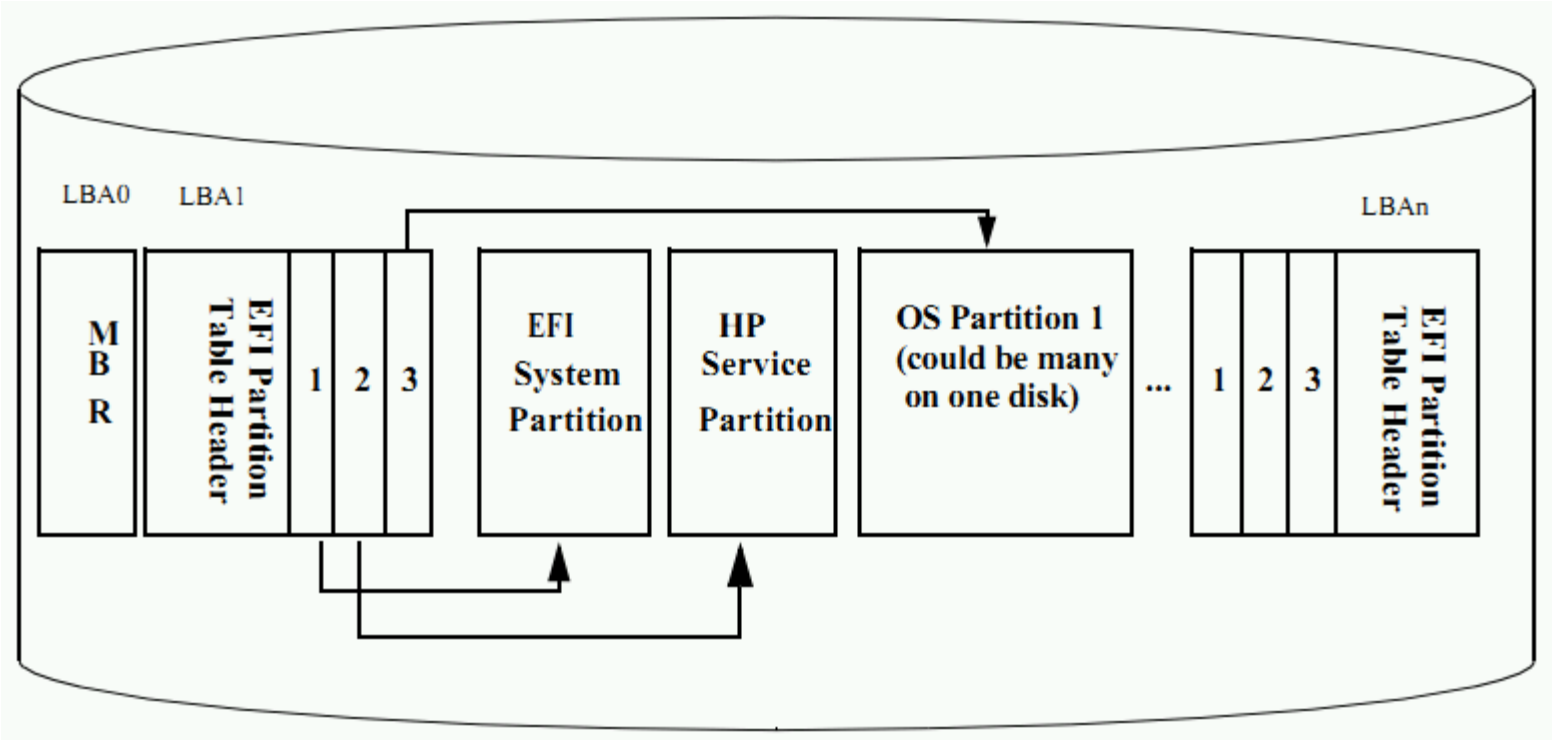


PDV SYSTEME hochformante IT®

Booting under EFI

- A bootable disk contains an EFI system partition
  - FAT file system
  - Directory `\EFI`
  - `\startup.nsh` is executed automatically
- Subdirectories of `\EFI` for OS bootloaders and utilities, e.g.
  - OpenVMS `\EFI\VMS\VMS_LOADER.EFI`
  - HP-UX `\EFI\HPUX\HPUX.EFI`
  - DVD boot `\EFI\BOOT\BOOTIA64.EFI`
- Administering Boot Manager selections
  - EFI shell command `bcfg`
  - EFI program `vms_bcfg` (on an OpenVMS boot disk)
  - Boot Manager configuration menu
  - OS utility
    - OpenVMS: SYS$MANAGER:BOOT_OPTIONS.COM

GPT formatted bootable disk



Agenda

- Intel Itanium and HP Integrity Server
- Consoles of HP Integrity Servers
- The Management Processor
- The Extensible Firmware Interface (EFI)
- **The EFI Shell**
- Examples of EFI Commands

Accessing the EFI Shell

- Power on Integrity - `MP:CM> PC -ON`
- Connect to system console - `MP> CO`
  - ↓ self test
  - ↓ configures devices
  - ↓ loads drivers
  - ↓ Boot Manager
    - Selection „Built-In Shell“ or „s/S“

EFI Shell: General

- Many (all?) commands support the option **-b** for paging output
- Command help
- Commands are grouped into classes:
  - boot
    - Booting options and disk-related commands
  - configuration
    - Changing and retrieving system information
  - device
    - Getting device, driver and handle information
  - memory
    - Memory related commands
  - shell
    - Basic shell navigation and customization
  - scripts
    - EFI shell-script commands

EFI Shell – Command help

```
Shell> help
List of classes of commands:
boot          -- Booting options and disk-related commands
configuration -- Changing and retrieving system information
device        -- Getting device, driver and handle information
memory        -- Memory related commands
shell         -- Basic shell navigation and customization
scripts       -- EFI shell-script commands
Use 'help <class>' for a list of commands in that class
Use 'help <command>' for full documentation of a command
Use 'help -a' to display list of all commands
```

EFI Shell – Command class boot

```
Shell> help boot
autoboot    -- View or set autoboot timeout variable
bcfg        -- Displays/modifies the driver/boot configuration
boottest    -- Set/View BootTest bits
clearlogs   -- Clears FPL and SEL logs
dblk        -- Displays the contents of blocks from a block
    device
lanboot     -- Performs boot over lan from EFI Shell
mount       -- Mounts a file system on a block device
reset       -- Resets the system
tftp        -- Tftp to a bootp/dhcp enabled unix boot server
vol         -- Displays volume information of the file system
```

EFI Shell – Command class configuration

```
Shell> help configuration
cpuconfig   -- Deconfigure or reconfigure cpus
date        -- Displays the current date or sets the systemdate
err         -- Displays or changes the error level
esiproc     -- Make an ESI call
errdump     -- View/Clear logs
info        -- Display hardware information
monarch     -- View or set the monarch processor
palproc     -- Make a PAL call
salproc     -- Make a SAL call
time        -- Displays the current time or sets the system time
ver         -- Displays the version information
```

EFI Shell – Command class device

```
Shell> help device
baud       -- Set serial port com settings
connect    -- Binds an EFI driver to a device and starts the driver
devices    -- Displays the devices being managed by EFI drivers
devtree    -- Displays the tree of devices of the EFI Driver Model
disconnect -- Disconnects one or more drivers from a device
dh         -- Displays the handles in the EFI environment
drivers    -- Displays the list of drivers of the EFI Driver Model
drvcfg     -- Invokes the Driver Configuration Protocol
drvdiag    -- Invokes the Driver Diagnostics Protocol
guid       -- Displays all the GUIDs in the EFI environment
lanaddress -- Display LAN MAC addresses
load       -- Loads and optionally connected EFI drivers
loadpcirom -- Loads a PCI Option ROM
map        -- Displays or defines mappings
openinfo   -- Displays the protocols on a handle and the agents
optload    -- Lists all optional ROM-based efi drivers and apps
pci        -- Displays PCI devices or PCI function config space
reconnect  -- Reconnects one or more drivers from a device
unload     -- Unloads a protocol image
```

EFI Shell – Command class memory

```
Shell> help memory
default     -- Sets, Resets, or Clears default NVM values
dmpstore    -- Displays all NVRAM variables
dmem        -- Displays the contents of memory
memmap      -- Displays the memory map
mm          -- Displays or modifies MEM/IO/PCI
pdt         -- View or set page deallocation table
```

EFI Shell – Command class shell

```
Shell> help shell
alias          -- Displays, creates, or deletes aliases in the EFI shell
attrib         -- Displays or changes the attributes of files or directories
cd             -- Displays or changes the current directory
cls            -- Clears the standard output with an optional background color
comp           -- Compares the contents of two files
cp             -- Copies one or more files/directories to another location
edit           -- Edits an ASCII or UNICODE file in full screen
eficompress    -- Compress a file
efidecompress  -- Compress a file
exit           -- Exits the EFI Shell
help           -- Displays help menus, command list, or verbose help of a command
hexedit        -- Edits with hex mode in full screen
ls             -- Displays a list of files and subdirectories in a directory
mkdir          -- Creates one or more directories
mode           -- Displays or changes the mode of the console output device
mv             -- Moves one or more files/directories to destination
rm             -- Deletes one or more files or directories
set            -- Displays, creates, changes or deletes EFI environment variables
setsize        -- Sets the size of the file
touch          -- Updates time with current time
type           -- Displays the contents of a file
xchar          -- Turn on/off extended character features
```

EFI Shell – Command class script

```
Shell> help script
echo        -- Displays messages or turns command echoing on/off
for/endfor -- Executes commands for each item in a set of items
goto        -- Makes batch file execution jump to another
    location
if/endif    -- Executes commands in specified conditions
pause       -- Prints a message and suspends for keyboard input
stall       -- Stalls the processor for some microseconds
```

EFI Shell – BCH Commands

```
Shell> help bch
    COnfiguration          help bch co
    INformation            help bch in
    PAth                   help bch pa
    ScRool                 help bch sr
    SEArch                 help bch sea
    SERvice                help bch ser
    BOot                   help bch bo
    HElp                   help bch he
    RESET                  help bch reset
    MAin                   help bch ma
For more help on one of the commands above, at the prompt type:
help bch COMMAND
```

Agenda

- Intel Itanium and HP Integrity Server
- Consoles of HP Integrity Servers
- The Management Processor
- The Extensible Firmware Interface (EFI)
- The EFI Shell
- **Examples of EFI Commands**

EFI: System Information

```
Shell> help info
Display hardware information

INFO [target]

target : all, boot, cache, chiprev, cpu, fw, io, mem, sys, warning

Examples:
  * To display all info:
  Shell> info all

  * To display cpu info:
  Shell> info cpu

  * To display fw and boot info:
  Shell> info fw boot

Shell> info fw

FIRMWARE INFORMATION

   Firmware Revision: 2.31 [4411]

   PAL_A Revision: 7.31/5.37
   PAL_B Revision: 5.65

   SAL Spec Revision: 3.01
   SAL_A Revision: 2.00
   SAL_B Revision: 2.31

   EFI Spec Revision: 1.10
   EFI Intel Drop Revision: 14.61
   EFI Build Revision: 1.22

   POSSE Revision: 0.10

   ACPI Revision: 7.00

   BMC Revision 1.53
   IPMI Revision: 1.00
   SMBIOS Revision: 2.3.2a
   Management Processor Revision: E.03.32
```

EFI: Configuring CPUs

```
Shell> help cpuconfig
Deconfigure or reconfigure cpus

CPUCONFIG [module [on|off]]
CPUCONFIG [threads [on|off]]
CPUCONFIG [pstates [on|off]]

module  : Specifies which cpu module to configure
threads : Use to display info or configure threads
pstates : Use to display info or configure Power/Performance States (P-states)
on      : Specifies to reconfigure a cpu module, cpu threads, or enable P-states
off     : Specifies to deconfigure a cpu module, cpu threads, or disable P-states

Note:
   1. Cpu status will not change until next boot.
   2. Specifying a cpu number without a state will display
      configuration status.
…

Shell> cpuconfig

PROCESSOR MODULE INFORMATION

          # of                L3      L4      Family/
   CPU    Logical             Cache   Cache   Model          Processor
   Module CPUs     Speed      Size    Size    (hex.)   Rev   State
   ------ -------  --------   ------  ------  -------  ---   ------------
     0       2      1.6 GHz    9 MB    None    20/00    C2        Active
     1       2      1.6 GHz    9 MB    None    20/00    C2        Active

CPU threads are turned off.
```

EFI: Configuring the system console(s)

```
Shell> help conconfig

Configure console devices

CONCONFIG [index] [on | off | primary]

index   Specifies index of console to set as primary
on      Enables the specified console as a secondary console
off     Puts console into "Not Configured" (NC) state
primary Sets the specified console as primary

Note:
   1. Primary console setting will take effect after reboot
   2. P in status column indicates console is primary
   3. S in status column indicates console is secondary
   4. NC in status column indicates console is not configured
   5. If a disabled console is set to primary it will be enbled

Shell> conconfig

CONSOLE CONFIGURATION

  Index Primary Type    Device Path
  ----- ------- -----   ----------
    1      P    Serial  Acpi(HWP0002,PNP0A03,0)/Pci(1|2)
    2      NC   VGA     Acpi(HWP0002,PNP0A03,0)/Pci(4|0)
```

EFI Devices & Mappings

```
Shell> map
fs0 : Acpi(HWP0002,100)/Pci(1|0)/Scsi(Pun0,Lun0)/HD(Part1,Sig8E89981A-0B97-11D7-9C4C-AF87605217DA)
blk1: Acpi(HWP0002,100)/Pci(1|0)/Scsi(Pun0,Lun0)
blk2: Acpi(HWP0002,100)/Pci(1|0)/Scsi(Pun0,Lun0)/HD(Part1,Sig8E89981A-0B97-11D7-9C4C-AF87605217DA)
blk3: Acpi(HWP0002,100)/Pci(1|0)/Scsi(Pun0,Lun0)/HD(Part3,SigC9D7945C-0BA7-11D7-9B31-FBA1AECDAF7E)
```

`Acpi(HWP0002,100)`

Device type HWP0002 (= Logical Block Address (LBA) device)

PCI host number 100 ("ROPE“ = circuitry handling I/O for PCI; defines I/O card slot)

`Pci(1|0)`

device/slot number 1

function number 0

`Scsi(Pun0,Lun0)`

Pun: Physical Unit (SCSI address)

Lun: Logical Unit

`HD(Part`*X*`,Sig`*Y*`)`

Partition *X* on a disk with signature *Y*

`fs`*X*`:`

→ EFI has found a FAT partition

EFI Devices (cont.)

```
Shell> map fs*
Device mapping table
  fs0     :HardDisk - Alias hd39dvsaamxfagryjo281474976710656b blk0
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x5001438011374778,0x1000000000000)/-
       HD(1,GPT,3BA4B191-F8D0-11E0-83D0-AA000400FEFF)
  fs1     :HardDisk - Alias hd39dvsaamxfagryjo562949953421312b blk1
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x5001438011374778,0x2000000000000)/-
       HD(1,GPT,88D32451-FA3E-11E0-BFE5-AA000400FEFF)
  fs2     :HardDisk - Alias hd39dvsaamxfagryjo562949953421312d blk2
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x5001438011374778,0x2000000000000)/-
       HD(3,GPT,88D32450-FA3E-11E0-BFE6-AA000400FEFF)
  fs3     :HardDisk - Alias hd39dvsaamxfagryjs281474976710656b blk3
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x500143801137477C,0x1000000000000)/-
       HD(1,GPT,3BA4B191-F8D0-11E0-83D0-AA000400FEFF)
  fs4     :HardDisk - Alias hd39dvsaamxfagryjs562949953421312b blk4
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x500143801137477C,0x2000000000000)/-
       HD(1,GPT,88D32451-FA3E-11E0-BFE5-AA000400FEFF)
  fs5     :HardDisk - Alias hd39dvsaamxfagryjs562949953421312d blk5
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x0)/Fibre(0x500143801137477C,0x2000000000000)/-
       HD(3,GPT,88D32450-FA3E-11E0-BFE6-AA000400FEFF)
  fs6     :HardDisk - Alias hd40dvsaamxfagryjq281474976710656b blk6
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477A,0x1000000000000)/-
       HD(1,GPT,3BA4B191-F8D0-11E0-83D0-AA000400FEFF)
  fs7     :HardDisk - Alias hd40dvsaamxfagryjq562949953421312b blk7
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477A,0x2000000000000)/-
       HD(1,GPT,88D32451-FA3E-11E0-BFE5-AA000400FEFF)
  fs8     :HardDisk - Alias hd40dvsaamxfagryjq562949953421312d blk8
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477A,0x2000000000000)/-
       HD(3,GPT,88D32450-FA3E-11E0-BFE6-AA000400FEFF)
  fs9     :HardDisk - Alias hd40dvsaamxfagryju281474976710656b blk9
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477E,0x1000000000000)/-
       HD(1,GPT,3BA4B191-F8D0-11E0-83D0-AA000400FEFF)
  fsA     :HardDisk - Alias hd40dvsaamxfagryju562949953421312b blkA
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477E,0x2000000000000)/-
       HD(1,GPT,88D32451-FA3E-11E0-BFE5-AA000400FEFF)
  fsB     :HardDisk - Alias hd40dvsaamxfagryju562949953421312d blkB
           PcieRoot(0x30304352)/Pci(0x7,0x0)/Pci(0x0,0x1)/Fibre(0x500143801137477E,0x2000000000000)/-
       HD(3,GPT,88D32450-FA3E-11E0-BFE6-AA000400FEFF)
  fsC     :Removable HardDisk - Alias hd16a0b blkC
           PcieRoot(0x30304352)/Pci(0x2,0x0)/Pci(0x0,0x0)/Scsi(0x0,0x0)/-
       HD(1,GPT,06936371-FA38-11E0-84EF-AA000400FEFF)
  fsD     :Removable CDRom - Alias cd66d0a blkD
           PcieRoot(0x30304352)/Pci(0x1D,0x7)/USB(0x3,0x0)/CDROM(0x0)
```

EFI: Booting OpenVMS

```
Shell> map -fs
Device mapping table
  fs0   : Acpi(HWP0002,PNP0A03,0)/Pci(2|1)/Usb(0,0)/CDROM(Entry0)
  fs1   : Acpi(HWP0002,PNP0A03,400)/Pci(1|0)/Sas(Addr500000E113495222,Lun0)/-
          HD(Part1,Sig6800E111-0A13-11E1-9878-001A4B064BF0)
  fs2   : Acpi(HWP0002,PNP0A03,400)/Pci(1|0)/Sas(Addr500000E113495222,Lun0)/-
          HD(Part3,Sig6800E110-0A13-11E1-9879-001A4B064BF0)
  fs3   : Acpi(HWP0002,PNP0A03,400)/Pci(1|0)/Sas(Addr5000CCA00B2001A1,Lun0)/-
          HD(Part1,Sig55AE9AF1-1695-11E1-99A7-001A4B064BF0)

Shell> fs1:

fs1:\> cd efi\vms

fs1:\efi\vms> vms_loader -flags 0,0

    HP OpenVMS Industry Standard 64 Operating System, Version V8.3-1H1
    © Copyright 1976-2009 Hewlett-Packard Development Company, L.P.

...
```

- EFI partitions within an OpenVMS system disk:

  SYS$LOADABLE_IMAGES:SYS$EFI.SYS

  SYS$MAINTENANCE:SYS$DIAGNOSTICS.SYS

- Beware of HBVS and shared system disks!

`Shell> drivers`

lists drivers loaded

column DRV: “Driver Handle“

column CFG has an `X`

→ driver supports the configuration protocol

column #D: number of devices managed

`Shell> drvcfg drv_hdl`

lists devices/controllers managed by *drv_hdl*

→ controller handle

`Shell> drvcfg -s drv_hdl [ctl_hdl]`

configures the device *drv_hdl* / *ctl_hdl*

Example: Switching a USB keyboard to german layout

```
Shell> drivers
            T   D
D           Y C I
R           P F A
V  VERSION  E G G #D #C DRIVER NAME                              IMAGE NAME
== ======== = = = == == ================================== ==================
…
23 00001010 ? X -  1  1 Usb Keyboard Driver                     UsbKb
…
Shell> drvcfg -s 23
Set Configuration Options
=========================================
    USB Keyboard Language Configuration
=========================================
  0. U.S. English
  1. Europe - English w/ Euro
  2. German
…
Current language selection = 0
Please enter a number followed by a <CR> : 2
New Keyboard Language = 2
  Drv[23]  Ctrl[ALL]  Lang[eng] - Options set.  Action Required is none
```

Example: Accessing a FC boot device

```
Shell> drivers
            T   D
D           Y C I
R           P F A
V  VERSION  E G G #D #C DRIVER NAME                          IMAGE NAME
== ======== = = = == == ================================== ==================
…
28 00000109 B X X  1  8 HP 4 Gb Fibre Channel Driver        PciROM:06:00:01:003
29 00000109 B X X  1  8 HP 4 Gb Fibre Channel Driver        PciROM:06:00:00:003
…
Shell> drvcfg 28
Configurable Components
  Drv[28]  Ctrl[2C]  Lang[eng]

Shell> drvcfg -s 28 2c
Set Configuration Options
  Drv[28]  Ctrl[2C]  Lang[eng]
Fibre Channel Driver Configuration Utility

NOTE: Do not redirect console output to a file.

Main Menu

 NVRAM Parameters
   1. Edit Adapter Settings
   2. Edit Advanced Settings
   3. Edit Database
   4. Edit Boot Settings
 Information
   5. Show Database
   6. Show Translation
   7. Show NVRAM Buffer
   8. Info
   9. Help
 Operation
  10. Abandon
  11. Write
  12. Quit

Enter a Selection:

…
```

Example: Accessing a FC boot device (cont.)

```
Enter a Selection: 4

Edit Boot Settings

  0. Previous Menu
  1. Help
  2. Enable Alternate Boot Device [n]
  3. Enable Selective Login [n]
  4. Enable Selective Lun Logins [n]
  5. OS Mode [HP-UX/OpenVMS]
  6. EFI Variable EFIFCScanLevel [?]
  7. Enable World Login [n]

Enter a Selection: 6

EFI Variable EFIFCScanLevel [?]? 1

Edit Boot Settings

  0. Previous Menu
  1. Help
  2. Enable Alternate Boot Device [n]
  3. Enable Selective Login [n]
  4. Enable Selective Lun Logins [n]
  5. OS Mode [HP-UX/OpenVMS]
  6. EFI Variable EFIFCScanLevel [1]
  7. Enable World Login [n]

Enter a Selection: 0

Main Menu
…
Enter a Selection: 12

Exiting...
  Drv[28]  Ctrl[2C]  Lang[eng] - Options set.  Action Required is None

Shell> reconnect -r
Shell> map –r –fs
```

Example: Accessing a FC boot device (cont.)

- After entering the FC boot device(s) into the Boot Manager, reset `EFIFCScanLevel` to 0

- With access to an OpenVMS EFI system partition (e.g. the installation DVD) the same can be accomplished using:

```
Shell> fsX:\efi\vms\vms_bcfg.efi boot fibre 1
Shell> reconnect -r
Shell> map -r –fs
```

VMS EFI Command vms_bfg

```
Shell> fsX:\efi\vms\vms_bcfg.efi

vms_bcfg driver|boot [add # device-name "desc"] [dump] –
         [rm #] [mv # #] [fibre #] [-v]

  driver  selects boot driver list

  boot    selects boot option list

  dump    [show] dumps selected list

  add     [set] add device-name with 'desc' at position #

  addp    [set] add 'file' with 'desc' at position #.
                  Use hard drive path

  addh    [set] add 'handle' with 'desc' at position #. Use Handle

  addv    [set] add 'D***:' with 'desc' at position #.
                  Use VMS device Name

  rm      [del] remove #

  mv      [ren] move # to #

  fibre   modifies EfiScanLevel to # (Default 0)

  -v      verbose
```

Example: Listing Boot Manager entries

```
Shell> fsX:\efi\vms\vms_bcfg.efi boot dump

The boot option list is:

01. Acpi(HPQ0002,400,PNP0A08)/Pci(0|0)/Pci(0|1)/-
          Fibre(WWN50001FE1500F90AF,Lun1000000000000)/-
          HD(Part1,Sig…)/\efi\vms\vms_loader.efi –
          "OpenVMS I64 V8.3-1H1 DGA11 FGB0.5000-1FE1-500F-90AF" OPT

…

08. Acpi(HPQ0002,400,PNP0A08)/Pci(0|0)/Pci(0|0)/-
          Fibre(WWN50001FE1500F90A8,Lun1000000000000)/-
          HD(Part1,Sig…)/\efi\vms\vms_loader.efi –
          "OpenVMS I64 V8.3-1H1 DGA11 FGA0.5000-1FE1-500F-90A8" OPT

09. VenHw(D65A6B8C-71E5-4DF0-A909-F0D2992B5AA9) "EFI Shell [Built-in]"

0A. Acpi(HWP0002,0,PNP0A03)/Pci(2|0)/Usb(0, 2) "iLO Virtual Media"

0B. Acpi(HWP0002,100,PNP0A03)/Pci(1|0)/Mac(001E0B5C06BE) "Core LAN Port 1"

0C. Acpi(HWP0002,100,PNP0A03)/Pci(1|1)/Mac(001E0B5C06BF) "Core LAN Port 2"

0D. Acpi(HWP0002,200,PNP0A03)/Pci(2|0)/Mac(001E0B5C06BC) "Core LAN Port 3"

0E. Acpi(HWP0002,200,PNP0A03)/Pci(2|1)/Mac(001E0B5C06BD) "Core LAN Port 4"

0F. Acpi(HWP0002,0,PNP0A03)/Pci(2|0)/Usb(0, 2)/CDROM(Entry0) –
          "Internal Bootable DVD"
```

Example: Creating Boot Manager entries

```
Shell> fsX:\efi\vms\vms_bcfg.efi boot addv 2 $1$dga3730 –
-fl 1,0 "DGA3730 Root 1"

VMS: DGA3730           Fibre Device
EFI: fs1: Acpi(000222F0,200)/Pci(1|1)/Fibre(…),Lun(D)
vms_bcfg: Add boot option as 2
vms_bcfg: Add the next available VMS path? (Yes/No) [YES]

VMS: DGA3730 Fibre Device
EFI: fs9: Acpi(000222F0,300)/Pci(1|0)/Fibre(…),Lun(D)
vms_bcfg: Add boot option as 3
vms_bcfg: Add the next available VMS path? (Yes/No) [YES]
```

Example: Listing OpenVMS device names

```
Shell> fsX:\efi\vms\vms_show.efi device

VMS: EWA0               00-1E-0B-5C-06-BE
EFI: Acpi(HWP0002,100,PNP0A03)/Pci(1|0)/Mac(001E0B5C06BE)

VMS: EWB0               00-1E-0B-5C-06-BF
EFI: Acpi(HWP0002,100,PNP0A03)/Pci(1|1)/Mac(001E0B5C06BF)

VMS: DKA-1              HP      DG072BABCE      HPD6
EFI: Acpi(HWP0002,200,PNP0A03)/Pci(1|0)/Sas(Addr500000E01C6E7B52)

VMS: DKA-1              HP      DG072BABCE      HPD6    V8_3_1H1
EFI: fs0: Acpi(HWP0002,200,PNP0A03)/Pci(1|0)/Sas(Addr500000E01C6EF042)

VMS: $1$DGA11           HP      HSV210          6220    V8_3_1H1
EFI: fs2: Acpi(HPQ0002,400,PNP0A08)/Pci(0|0)/Pci(0|0)/-
          Fibre(WWN50001FE1500F90AA,Lun1000000000000)

VMS: $1$DGA12           HP      HSV210          6220
EFI: Acpi(HPQ0002,400,PNP0A08)/Pci(0|0)/Pci(0|0)/-
          Fibre(WWN50001FE1500F90A8,Lun2000000000000)

…
```

EFI: Configuring TCP/IP (on an OpenVMS disk)

```
Shell> fs0:
fs0:\> cd \efi\vms\tools
fs0:\efi\vms\tools> type startup_net.nsh
File: fs0:\efi\vms\tools\startup_net.nsh, Size 702

load \efi\vms\tools\tcpipv4.efi
\efi\vms\tools\ifconfig lo0 inet 127.0.0.1 up
\efi\vms\tools\ifconfig sni0 inet <a.b.c.d> netmask <a.b.c.d> up
\efi\vms\tools\route add default <a.b.c.d>

fs0:\efi\vms\tools> edit startup_net.nsh
```

EFI: NVRAM backup

- HP EFI tool to save and restore the EFI NVRAM (boot configuration etc.)
- Download from HP‘s web site
  - Google search:
    “Integrity Non-Volatile RAM Configuration Back-up site:hp.com“
- Transfer `nvrambkp.efi` to the Integrity:
  - USB device
  - Configure and start TCP/IP, then use FTP
  - OpenVMS: SYS$SYSTEM:EFI$CP.EXE
    - OpenVMS Release Notes (since V8.2):

> Using EFI$CP Utility not Recommended
>
> The OpenVMS EFI$CP utility is presently considered undocumented and unsupported. HP recommends against using this utility. Certain privileged operations within this utility could render OpenVMS Integrity servers unbootable.

References

HP Integrity:

www.hp.com/go/integrity

www.hp.com/go/integrity_servers-docs

www.hp.com/go/blades-docs

VMS EFI Utilities:

HP OpenVMS System Management Utilities Reference Manual
Chapter 10: EFI Utilities for OpenVMS

MP Documentation:

HP Integrity iLO 2 MP Operations Guide
HP Integrity iLO 3 Operations Guide

POSSE Documentation:

<Integrity System> User Service Guide, Appendix “Utilities“

References

Intel Itanium:

www.intel.com/itcenter/products/itanium/

UEFI:

www.uefi.org

tianocore.org (OpenSource components)

Overview of MP commands:

h30499.www3.hp.com/hpeb/attachments/hpeb/hpsc-46/2037/1/MP.pdf

Q&A

PDV SYSTEME
hochformante IT®