

Overview

VSI OpenVMS Version 8.4-2L1 for Integrity Servers

Introduction

This QuickSpecs describes the VMS Software, Inc. (VSI) OpenVMS Operating System software for HPE Integrity servers.

Description

OpenVMS is a general-purpose, multiuser operating system that runs in both production and development environments. VSI OpenVMS software supports industry standards, facilitating application portability and interoperability. OpenVMS provides symmetric multiprocessing (SMP) support for multiprocessing systems.

The OpenVMS operating system can be tuned to perform well in a wide variety of environments. This includes combinations of compute-intensive, I/O intensive, client/server, real-time, and other environments. Actual system performance depends on the type of computer, available physical memory, and the number and type of active disk and tape drives. The OpenVMS operating system has well-integrated networking, distributed computing, client/server, multiprocessing, and windowing capabilities. It contains extensive features that promote ease-of-use, improve the productivity of programmers, and facilitate system management.

For information about the VSI OpenVMS Version 8.4-2L1 new features, see the *VSI OpenVMS Version 8.4-2L1 Cover Letter and Release Notes*. The following table describes the support status of VSI OpenVMS V8.4-2L1 with different server models, including HPE Integrity server models based on the Intel® Itanium® 9500 series processors. Customers are free to run VSI OpenVMS Version 8.4-2L1 on any server but should consult the following table for formal support status.

Overview

Supported Servers

OpenVMS V8.4-2L1 Server Support			
Server Model	VSI OpenVMS V8.4-2L1	VSI Technical Support	HPE Technical Support
rx2800 i4	Tested	Supported	Supported
BL860c i4	Tested	Supported	Supported
BL870c i4	Tested	Supported	Supported
BL890c i4	Tested	Supported	Supported
rx2800 i2	Tested	Supported	Supported
BL860c i2	Tested	Supported	Supported
BL870c i2	Tested	Supported	Supported
BL890c i2	Tested	Supported	Supported
rx1600	Tested	Supported	Not supported
rx2600	Tested	Supported	Not supported
rx2620	Tested	Supported	Not supported
rx2660	Tested	Supported	Not supported
rx3600	Tested	Supported	Not supported
rx6600	Tested	Supported	Not supported
rx7640	Tested	Supported	Not supported
rx8640	Tested	Supported	Not supported
HPE Integrity Superdome	Not tested	Not supported	Not supported

Upgrading to VSI OpenVMS V8.4-2L1

In addition to HPE OpenVMS V8.4 with Update 900, U1000, or U1100, VSI supports upgrades from earlier versions of OpenVMS. The following table describes the upgrade paths that VSI supports:

VSI OpenVMS V8.4-2L1 Upgrade Path Support	
Upgrade Target Version	VSI Technical Support
HPE Version v8.4 U900, U1000, or U1100	Supported
HPE Version v8.3-1H1	Supported
HPE Version v8.3	Supported
HPE Version v8.2-1	Not Supported

Standard Features

User Environment

Users can access the OpenVMS software by using the English-like DIGITAL Command Language (DCL), the command language for OpenVMS that is supplied with the system. DCL commands provide information about the system and initiate system utilities and user programs. DCL commands take the form of a command name followed by parameters and qualifiers.

Users can enter DCL commands at a terminal or include them in command procedures. These command procedures can be run interactively or submitted to a batch queue for later processing. Information about DCL and OpenVMS utilities is available on line through the OpenVMS Help system.

For users who are familiar with the UNIX shell and utilities, an open source port of GNV is available. GNV implements a UNIX environment on OpenVMS and includes an Implementation of the UNIX shell BASH (Bourne Again Shell) and many UNIX-shell utilities.

The following tools and utilities are integrated into the OpenVMS operating system.

Text Processing

The Extensible Versatile Editor (EVE) is the default editor for OpenVMS. EVE allows users to insert, change, and delete text quickly. EVE is a full-screen editor that allows users to scroll through text on a terminal screen. EVE provides an EDT-style keypad, allowing EDT users to move easily to EVE.

Mail Utility

The Mail utility allows users to send messages to any other user on the system. Multinode operation is available if a DECnet or TCP/IP product is installed and licensed on each participating node on the network.

Command Level Programming

Command-level programming allows users to create special files, called command procedures that contain a series of DCL commands. When users execute a command procedure, the system processes the commands in the command procedure consecutively.

User Environment Tailoring

Users can customize the computing environment with login command procedures, shorthand commands, binding of commands to function keys, and command recall and editing.

Program Development Environment

OpenVMS includes a comprehensive set of tools for developing programs, including: run-time libraries (RTLs), a linker, a librarian, and a symbolic debugger. The following tools are available to the OpenVMS programmer.

Standard Features

Language and Run-Time Library Support

OpenVMS includes several RTLs that provide:

- String manipulation
- Parallel processing support
- I/O routines
- I/O conversion
- Terminal-independent screen handling
- Date and time formatting routines
- Highly accurate mathematical functions
- Signaling and condition handling
- Other general-purpose functions

With OpenVMS for Integrity servers, these routines can be called from programs written in such languages as MACRO-32, BASIC, C, C++, COBOL, Fortran, and Pascal.

Also included in OpenVMS are language-support libraries. While each language is different, all provide support for sequential file I/O, and most support direct and indexed file I/O. Language RTLs also provide support for I/O formatting, error handling, and in Fortran, the ability to read unformatted files that contain data from other vendors

RTLs are provided to support translated images created from user-mode images built on OpenVMS Alpha Version 6.1 through Version 7.3-2.

Calling Standard

All OpenVMS programming languages comply with the OpenVMS Calling Standard. This means that routines written in any of these languages can directly call routines written in any other language. Development of applications using multiple languages is simple and straightforward.

All user-accessible routines in the RTLs follow the appropriate platform calling standard and condition-handling conventions, and most are contained within shareable images.

At a lower level, programs can call system services directly for security, event flag, asynchronous system trap, logical name, record and file I/O, process control, timer, time conversion, condition handling, lock management, and memory management. Again, system services use the appropriate platform calling standard and condition-handling conventions.

OpenVMS supports the execution of user-mode images created on earlier versions of OpenVMS. Typically, recompiling and relinking are not required.

MACRO Compiler

With minor modifications, VAX MACRO-32 sources can be compiled for execution on Integrity servers.

Standard Features

POSIX Threads Library

OpenVMS includes a user-mode, multithreading capability called POSIX Threads Library. POSIX Threads Library provides a POSIX 1003.1-1996 standard style threads interface. Additionally, POSIX Threads Library provides an interface that is the OpenVMS implementation of Distributed Computing Environment (DCE) threads as defined by The Open Group.

POSIX Threads Library is a library of run-time routines that allows the user to create multiple threads of execution within a single address space. With POSIX Threads Library Kernel Threads features enabled, POSIX Threads Library provides for concurrent processing across all CPUs by allowing a multithreaded application to have a thread executing on every CPU (on both symmetric and asymmetric multiprocessor systems). Multithreading allows computation activity to overlap I/O activity. Synchronization elements, such as mutexes and condition variables, are provided to help ensure that shared resources are accessed correctly. For scheduling and prioritizing threads, POSIX Threads Library provides multiple scheduling policies. For debugging multithreaded applications, POSIX Threads Library is supported by the OpenVMS Debugger. POSIX Threads Library also provides Thread Independent Services (TIS), which assist in the development of threadsafe APIs.

Librarian Utility

The Librarian utility permits storage of object modules, image files, macros, help files, text files, or any general record-oriented information in central, easily accessible files. Object module and image file libraries are searched by the linker when the linker finds a reference it cannot resolve in one of its input files. Macro libraries are searched by MACRO-32 and MACRO-64 when either finds a macro name that is not defined in the input file.

Hypersort

Hypersort is a portable library of user-callable routines that provide a high-performance sorting capability for Integrity servers.

Traceback Facility

The Traceback facility is a debugging tool that provides symbolic information about call stack PCs. When an application is compiled and linked with traceback information, the Traceback facility translates stack frame addresses into routine names and line numbers and displays a symbolic traceback whenever a runtime error occurs in that application.

Debugger

The OpenVMS Debugger allows users to trace program execution, as well as display and modify register contents using the same symbols that are present in the source code. The debugger contains a heap analyzer feature that displays a graphic view of memory allocations and deallocations in real time.

Standard Features

System Code Debugger

The OpenVMS System Code Debugger is a kernel code debugger. It allows a system code developer to trace the execution of nonpageable system code at any interrupt priority level (IPL). Based on the OpenVMS Debugger, the System Code Debugger uses the same interface and most of the same command set.

System Dump Analyzer (SDA) Utility

In the event of a system failure, OpenVMS writes the contents of memory to a preallocated dump file. This dump file can later be analyzed using System Dump Analyzer (SDA). System dumps can either be full memory dumps, where all memory is written, or selective memory dumps, where only portions of memory in use at the time of the system failure are written. The dump file can be located on any locally connected disk. On Integrity servers, dump compression allows both full and selective dumps to be written to smaller files than required for uncompressed dumps. Full memory dumps, if not compressed, require a dump file big enough to hold all memory. Selective memory dumps write as much of the memory in use at the time of the system failure that will fit into the dump file.

Spinlock Tracing Utility

The Spinlock Tracing Utility provides a mechanism to characterize spinlock usage and collect performance data for a given spinlock on a per-CPU basis. It can identify which spinlock is heavily used and what process is acquiring and releasing spinlocks.

Process Dumps

When an application fails, a copy of its registers and memory can be written to a data file, which can be examined using the ANALYZE PROCESS utility. This utility uses the same interface and commands as the OpenVMS Debugger to allow registers and memory to be examined. On Integrity servers, another process can initiate the writing of the memory dump.

RMS File Utilities

Record Management Services (RMS) file utilities allow users to analyze the internal structure of an RMS file and tune the I/O, memory, space and performance parameters of the file. The RMS file utilities can also be used to create, load, and reclaim space in an RMS file. For more information about RMS, see the Operating System Environment section of this QuickSpecs.

File Differences Utility

This utility compares the contents of two files and lists those records that do not match.

Translated Image Environment (TIE) (Integrity servers)

OpenVMS for Integrity servers provides an array of services that allow the operation of programs that have undergone binary translation from OpenVMS Alpha images or VESTed OpenVMS VAX images. These programs perform virtually all user-mode functions on OpenVMS for Integrity servers and operate in combination with other programs (images) that have been translated from OpenVMS Alpha or VAX, or have been built using native compilers on OpenVMS for Integrity servers. Without requiring special source code, the TIE resolves differences between the Alpha and Integrity architectures, including floating-point.

Note: Binary translation is a means of moving complex software application executable images, where source code is not available, from one architecture and operating system to another architecture and operating system.

Standard Features

System Management Environment

OpenVMS provides a set of tools and utilities that aid the system manager in configuring and maintaining an optimal system as follows:

Web-Based Enterprise Management Services for OpenVMS

Web-Based Enterprise Management (WBEM) Services for OpenVMS is an industry standard for monitoring and controlling resources. It is available and installed automatically with OpenVMS on Integrity server systems. WBEM Services for OpenVMS (WBEMCIM) is required for use of such features as HPE Systems Insight Manager (HPE SIM). In addition, WBEM Providers for OpenVMS is installed automatically with OpenVMS for Integrity servers.

For server blade support, "Providers" are included that enable the monitoring of hardware and the operating system, including:

- Operating system
- Computer system
- Process and processor statistics
- Indication (monitors events)
- Firmware version
- Fan and power supply
- Management Processor
- CPU instance
- Memory instance
- Enclosure

VSI Availability Manager

VSI Availability Manager is a system management tool that enables you to monitor one or more OpenVMS nodes on an extended local area network (LAN) from either an OpenVMS Alpha system, or an OpenVMS for Integrity server system, or a PC running Windows. This tool helps system managers and analysts target a specific node or process for detailed analysis and also can resolve certain performance or resource problems. It is the multiplatform replacement for the DECams product and includes the DECams functionality in its capabilities.

Availability Manager has a wide-area capability whereby any system on the network supporting Availability Manager can be managed from a central console. Moreover, Availability Manager is enhanced to support Cluster over IP to manage and monitor LAN or IP path data, and IP interface for cluster communication.

The Data Collector, part of the Availability Manager product, collects system and process data on an OpenVMS node and should be installed on each node that you need to monitor (Alpha and Integrity servers).

The Data Analyzer analyzes and displays the data collected by the Data Collector, and can analyze and display data from many OpenVMS nodes simultaneously (OpenVMS Alpha nodes, and PCs running Windows).

Class Scheduler for CPU Scheduling

The Class Scheduler has a SYSMAN-based interface for defining and controlling scheduling classes for OpenVMS systems that allows you to designate the percentage of CPU time that a system's user may receive by placing users into scheduling classes.

Standard Features

Batch and Print Queuing System

OpenVMS provides an extensive batch and print capability that allows the creation of queues and the setup of spooled devices to process non-interactive workloads in parallel with timesharing or real-time jobs. The OpenVMS batch and print operations support two types of queues: generic queues and execution queues. A generic queue is an intermediate queue that holds a job until an appropriate execution queue becomes available to initiate the job. An execution queue is a queue through which the job (either print or batch) is actually processed. Because multiple execution queues can be associated with a generic queue, OpenVMS enables load balancing across available systems in an OpenVMS Cluster system, increasing overall system throughput. Print queues, both generic and execution, together with queue management facilities, provide versatile print capabilities, including support for various print file formats.

Accounting Utility

For accounting purposes, OpenVMS keeps records of system resource usage. Statistics include processor and memory utilization, I/O counts, print symbiont line counts, image activation counts, and process termination records. The OpenVMS Accounting utility allows you to generate reports using this data. Use the reports to learn more about how the system is used and how it performs.

Audit Analysis Utility

For security auditing purposes, OpenVMS selectively records critical, security-relevant events in the system security audit log file. These records contain the date and time the event occurred, the identity of the associated user process, and information specific to each event type. This information helps the system manager maintain system security and deter possible intruders. The OpenVMS Audit Analysis utility allows you to generate various reports from this data.

Autoconfigure and AUTOGEN Utilities

The Autoconfigure and AUTOGEN utilities automatically configure the available devices in the system tables and set system parameters based on the peripheral and memory architecture. This eliminates the need for a traditional system generation process when the hardware configuration is expanded or otherwise modified. The OpenVMS AUTOGEN command procedure sets several system parameters automatically by detecting the devices installed in a configuration. A feedback option allows you to generate a report of recommended parameter settings based on previous usage patterns. Use AUTOGEN to adjust system parameters to match your system's workload for optimum system performance.

Backup Utility

The Backup utility provides both full-volume and incremental file backups for file-structured, mounted volumes and volume sets. Individual files, selected directory structures, or all files on a volume set can be backed up and restored. Files can be selected by various dates (such as creation or modification) and can be backed up to magnetic tape, magnetic disk, or Write Once Read Many (WORM) optical disk. The Backup utility can also be used to restore a saveset or list the contents of a saveset.

The Backup utility supports volumes up to 2 TB. The Backup utility has also been enhanced to create and restore a compressed save set, which can be created on disks and magnetic tapes. The compression ratio depends on the data content in the files. A Backup API is included for invoking backup routines from an executable procedure.

The Backup Manager for OpenVMS provides a screen-oriented interface to the Backup utility that assists users in performing routine backup operations. The Backup Manager is menu driven and provides:

- Access to the save, restore, and list operations without having to understand Backup command syntax
- The ability to create, modify, recall, and delete Backup Manager templates that describe the Backup save operations

Standard Features

Recordable CD and DVD

On Integrity server systems, OpenVMS provides the capability to record locally mastered disk volumes or disk image files onto a CD-R, CD-RW, DVD+R, or DVD+RW optical-media recording device on specific drives and configurations. On supported Alpha systems and supported Integrity server systems that ship with writable CD devices (CD-RW), OpenVMS provides the capability to write once to CD-R media using an application shipping in the base operating system. For application details, please refer to the OpenVMS documentation set.

Analyze Disk Structure Utility

The Analyze Disk Structure utility compares the structure information on a disk volume with the contents of the disk, prints the structure information, and permits changes to that information. It can also be used to repair errors detected in the file structure of disks.

License Management Facility (LMF)

The License Management Facility allows the system manager to enable software licenses and to determine which software products are licensed on an OpenVMS system.

System Management Utility (SYSMAN)

The System Management utility allows system managers to define a management environment in which operations performed from the local OpenVMS system can be executed on all other OpenVMS systems in the environment.

Security

OpenVMS provides a rich set of tools to control user access to system-controlled data structures and devices that store information. OpenVMS employs a reference monitor concept that mediates all access attempts between subjects (such as user processes) and security-relevant system objects (such as files). OpenVMS also provides a system security audit log file that records the results of all object access attempts. The audit log can also be used to capture information regarding a wide variety of other security-relevant events.

User account information, privileges and quotas associated with each user account is maintained in the system user authorization file (SYSUAF). Each user account is assigned a user name, password, and unique user identification code (UIC). To log in and gain access to the system, the user must supply a valid user name and password. The password is encoded and does not appear on terminal displays. Users can change their password voluntarily, or the system manager can specify how frequently passwords change, along with minimum password length, password history policy, and the use of randomly generated passwords.

Operations

OpenVMS allows for varying levels of privilege to be assigned to different operators. Operators can use the OpenVMS Help Message utility to receive online descriptions of error messages. In addition, system-generated messages can be routed to different terminals based on their interest to the console operators, tape librarians, security administrators, and system managers.

Security auditing is provided for the selective recording of security-related events. This auditing information can be directed to security operator terminals (alarms) or to the system security audit log file (audits). Each audit record contains the date and time of the event, the identity of the associated user process, and additional information specific to each event.

OpenVMS provides security auditing for the following events:

- Login and logout
- Login failures and break-in attempts
- Object creation, access, deaccess, and deletion; selectable by use of privilege, type of access, and on individual objects
- Authorization database changes
- Network logical link connections for DECnet for OpenVMS, DECnetPlus, DECwindows, IPC, and SYSMAN
- Use of identifiers or privileges
- Installed image additions, deletions, and replacements

Standard Features

- Volume mounts and dismounts
- Use of the Network Control Program (NCP) utility
- Use or failed use of individual privileges
- Use of individual process control system services
- System parameter changes
- System time changes and recalibrations

Every security-relevant system object is labeled with the UIC of its owner along with a simple protection mask. The owner UIC consists of two fields: the user field and a group field. System objects also have a protection mask that allows read, write, execute, and delete access to the object's owner, group, privileged system users, and to all other users. The system manager can protect system objects with access control lists (ACLs) that allow access to be granted or denied to a list of individual users, groups, or identifiers. ACLs can also be used to audit access attempts to critical system objects.

OpenVMS applies full protection to the following system objects:

- Common event flag cluster
- Devices
- Files
- Group global sections
- Logical name tables
- Batch/print queues
- Resource domains
- Security classes
- System global sections
- ODS-2 volumes
- ODS-5 volumes

OpenVMS provides optional security solutions to protect your information and communications:

- OpenVMS includes encryption for data confidentiality that ships as part of the operating system, thereby removing the requirement to license and install Encrypt separately. The ENCRYPT and DECRYPT commands, now part of OpenVMS, support AES file encryption with 128, 192, or 256 bit keys. AES encryption is also supported by BACKUP/ENCRYPT, allowing for the creation of encrypted tapes and save-sets. The built-in encryption functionality is backward-compatible with file and backup tapes created by the former layered product Encryption for OpenVMS. This layered product featured 56-bit Data Encryption Standard (DES), which continues to function today, allowing for the decryption of archived DES encrypted data. The AES encryption functionality supports Electronic Code Book (ECB) and Cipher Block Chaining (CBC) block modes of encryption. The Cipher Feedback (CFB) and Output Feedback (OFB) 8-bit character stream modes are also supported from the command line as well as by the programmatic APIs.
- Secure Sockets Layer1 (SSL1) for OpenVMS Integrity server systems provides secure transfer of sensitive information over the Internet
- Common Data Security Architecture (CDSA) is configured and initialized automatically during installation and upgrades and is required for Secure Delivery purposes and other security features. If you install a newer version of CDSA without upgrading the base operating system, you must initialize the CDSA software, using the following command. Enter the command from an account that has both SYSPRV and CMKRNL privileges (for example, the SYSTEM account). `$ SYS$STARTUP:CDSA$UPGRADE`
- Kerberos for OpenVMS
- Per-Thread Security Profiles
- External Authentication
- Global and Local Mapping of LDAP users
- VSI Code Signing for OpenVMS: OpenVMS kits will be signed using VSI Code Signing Service

NOTE: Users who are externally authenticated by their LAN Manager need only remember a single user name/password combination to gain access to their OpenVMS and LAN Manager accounts.

Standard Features

NOTE: Because no system can provide complete security, VSI cannot guarantee complete system security. However, VSI continues to enhance the security capabilities of its products. Customers are strongly advised to follow all industry-recognized security practices. Recommended procedures are described in the *OpenVMS Guide to System Security*.

Operating System Environment

Processes and Scheduling

Executable images consist of system programs and user programs that have been compiled and linked. These images run in the context of a process on OpenVMS systems. Sixty-four process priorities are recognized on OpenVMS for Integrity servers. Priorities 0 to 15 are for time-sharing processes and applications (four is the typical default for timesharing processes). Priorities 16 to 63 on Integrity servers are for real-time processes. Real-time processes can be assigned higher priorities to ensure that they receive processor time whenever they are ready to execute. OpenVMS uses paging and swapping to provide sufficient virtual memory for concurrently executing processes. Paging and swapping is also provided for processes whose memory requirements exceed available physical memory.

64-Bit Virtual Addressing

OpenVMS provides support for 64-bit virtual memory addressing. This capability makes the 8 TB virtual address space available to the OpenVMS operating system and to application programs. Future hardware implementations for Integrity servers will provide greater capacity. OpenVMS applications can take advantage of 64-bit processing by using 64-bit data types supported by the compilers. For further details, see the SPDs for the OpenVMS for Integrity servers compilers.

Very Large Memory (VLM) Features

OpenVMS for Integrity servers provide the following additional memory management VLM features beyond those provided by 64-bit virtual addressing. These features can be used by database servers to keep large amounts of data in memory, resulting in dramatically increased runtime performance. The VLM features provided by OpenVMS for Integrity servers are:

- Memory-resident global sections
- Fast I/O for global sections
- Shared page tables
- Expandable global page table
- Reserved memory registry

DECdtm Services

DECdtm services embedded in the OpenVMS operating system support fully distributed databases using a two-phase commit protocol. DECdtm services provide the technology and features for distributed processing, ensuring transaction and database integrity across multiple resource managers. Updates to distributed databases occur as a single all-or-nothing unit of work, regardless of where the data physically resides. This ensures the consistency of distributed data. DECdtm services allow applications to define global transactions that can include calls to any number of VSI data management products. Regardless of the mix of data management products used, the global transaction either commits or aborts. OpenVMS is unique in providing transaction processing functionality with base operating system services.

DECdtm features include:

- Embedded OpenVMS system services that support the DECtp architecture, providing the features and technology for distributed transaction processing.
- Ability for multiple disjoint resources to be updated automatically. These resources can be either physically disjointed on different clusters at separate sites, or logically disjointed in different databases on the same node.
- Ability to use the X/Open Distributed Transaction Processing XA interface that enables the DECdtm transaction manager to coordinate XA-compliant resource managers (the DECdtm XA Veneer), and XA-compliant transaction processing systems to coordinate DECdtm-compliant resource managers (the DECdtm XA Gateway).
- Robust application development. Applications can be written to ensure that data is never in an inconsistent state, even in the event of system failures.
- Ability to be called using any HPE TP monitor or database product. This is useful for applications using several HPE database products.

Standard Features

Interprocess Communication

OpenVMS provides the following facilities for applications that consist of multiple cooperating processes:

- Mailboxes as virtual devices that allow processes to communicate with queued messages.
- Shared memory sections on a single processor or an SMP system that permit multiple processes to access shared address space concurrently.
- Common event flags that provide simple synchronization.
- A lock manager that provides a more comprehensive enqueue/dequeue facility with multilevel locks, values, and asynchronous system traps (ASTs).
- Intracluster communication services through which two processes running on the same system or on different OpenVMS Cluster nodes can establish a connection and exchange data.
- Logical names through which one process can pass information to other processes running on the same system or on different OpenVMS Cluster nodes.
- Network interprocess communication is available via TCP/IP Services and DECnet-Plus (product licenses are required).

Symmetric Multiprocessing (SMP)

OpenVMS provides symmetric multiprocessing (SMP) support for Integrity servers multiprocessor systems. SMP is a form of tightly coupled multiprocessing in which all processors perform operations simultaneously. All processors perform operations in all OpenVMS access modes, user, supervisor, executive, and kernel.

OpenVMS SMP configurations consist of multiple CPUs executing code from a single shared memory address space. Users and processes share a single copy of OpenVMS for Integrity servers address space. SMP also provides simultaneous shared access to common data in global sections to all processors. OpenVMS SMP selects the CPU where a process will run based on its priority and in special cases as directed by the application. OpenVMS uses a specialized scheduling algorithm when running a nonuniform memory access (NUMA) platform.

SMP support is an integral part of OpenVMS and is provided to the user transparently. Because an SMP system is a single system entity, it is configured into a network and OpenVMS Cluster configurations as a single node.

VSI OpenVMS V8.4-2L1 supports a maximum of 32 cores in an instance of the operating system.

Networking Facilities

OpenVMS provides device drivers for all local area network (LAN) adapters listed in the LAN Options section of Appendix A of this document. Application programmers can use the QIO system service to communicate with other systems connected via the LAN using either Ethernet or Institute of Electrical and Electronics Engineers (IEEE) 802.3 packet format. Simultaneous use of VSI Ethernet and the IEEE 802.3 protocols are supported on any HPE LAN adapter.

OpenVMS supports the following networking products:

- VSI TCP/IP Services for OpenVMS, the industry-standard set of protocols for interoperating between different operating systems
- VSI DECnet-Plus, the Digital Network Architecture, Phase V
- VSI DECnet, the DIGITAL Network Architecture, Phase IV

These networking products are described in this QuickSpec under Associated Products.

Terminal Server Products

Terminal server products provide network access to OpenVMS from terminal (serial) based devices. When used in an OpenVMS Cluster environment, terminal servers distribute users across the available Integrity server systems at login time. OpenVMS can also establish a connection to other devices (such as printers) attached to such terminal servers.

Universal Serial Bus Support

OpenVMS supports the Universal Serial Bus (USB) technology. Support for the USB interconnect enables OpenVMS

Standard Features

systems to connect to multiple supported USB devices using a single USB cable. OpenVMS supports one USB keyboard and mouse on systems that are supported by OpenVMS and have USB hardware and a graphics controller. Serial support is provided through the USB serial multiplexer (MUX). OpenVMS supports several generic chipsets which allow third-party USB-based serial multiplexers to connect to OpenVMS systems for RS232 serial lines, traditional terminal connections, and low-speed system-to-system connectivity.

OpenVMS provides a USB configuration tool called UCM that can be used to track USB configuration changes like plug and unplug events. UCM can also be used to restrict the automatic addition of specific devices and classes of devices. The UCM event log is used by VSI to help diagnose problems with USB devices. OpenVMS supports USB low-, full-, and high-speed devices for all supported OpenVMS Integrity systems. Support includes both reading and burning DVDs on the following supported Integrity server systems: rx2660, rx2800i2, rx2800i4, rx3600, rx6600.

Reliability

OpenVMS handles hardware errors as transparently as possible while maintaining data integrity and providing sufficient information to diagnose errors. The system limits the effects of an error by first determining if the error is fatal. If the error occurs in system context, the OpenVMS system shuts down. If the error is nonfatal, the system recovers actions pertinent to the error and continues the current operation. In all cases, information relevant to the error is written to the error log file for later analysis. Hardware errors include the following categories:

- **Processor errors.** These include processor hard or soft errors, processor machine checks, and adapter errors.
- **Memory errors.** These can be unrecoverable (hard) errors or recoverable (soft) errors. The system examines memory at startup time and does not use any bad pages. During system operation, the system corrects all single-bit memory errors for those systems with error correction code (ECC) memory.
- **Correctible memory errors.** A primary cause of these correctible memory errors is alpha particle radiation. On some processors, when correctible memory errors occur, the memory controller corrects only the data returned to the CPU or I/O controller. The actual data in memory is left with the error intact. Subsequent read operations cause correction cycles to occur and, in most cases, an interrupt to report the error. On many of these processors, OpenVMS monitors the occurrence of correctible memory errors and, in almost all cases, removes the error condition by rewriting the data in memory. This causes the data to be corrected in that memory location.

Other failures include:

- Operating system errors (system-detected inconsistencies or architectural errors in system context)
- User errors
- I/O errors

The system logs all processor errors, all operating system errors detected through internal consistency checks, all double-bit memory errors (and a summary of corrected single-bit memory errors), and most I/O errors. If the system is shut down because of an unrecoverable hardware or software error, a dump of physical memory is written. The dump includes the contents of the processor registers. Use the OpenVMS System Dump Analyzer (SDA) utility to analyze memory dumps.

OpenVMS supports CPU Component Indictment, also called Dynamic Processor Resilience (DPR). When certain error conditions persist a CPU will be stopped and no longer used by the running system. Use of this feature is controlled by the System Manager via `SYS$MANAGER:SYS$INDICTMENT_POLICY.COM`.

Input/Output

The QIO system service and other related I/O services provide a direct interface to the operating system's I/O routines. These services are available from within most OpenVMS programming languages and can be used to perform low-level I/O operations efficiently with a minimal amount of system overhead for time-critical applications.

Device drivers execute I/O instructions to transfer data to and from a device and to communicate directly with an I/O device. Each type of I/O device requires its own driver. VSI supplies drivers for all devices supported by the OpenVMS operating system and provides QIO system service routines to access the special features available in many of these devices.

OpenVMS supports a variety of disk and tape peripheral devices, as well as terminals, networks, and mailboxes (virtual

Standard Features

devices for interprocess communication), and more general I/O devices.

I/O Performance Features

Fast I/O provides a suite of additional system services that applications can use to improve I/O throughput. The fast I/O services minimize the CPU resources required to perform I/O.

Fast Path provides a streamlined mainline code path through the I/O subsystem to improve both uniprocessor and multiprocessor I/O performance. On multiprocessor systems, Fast Path allows all CPU processing for specific I/O adapters to be handled by a specific CPU. This can significantly lower the demands on the primary CPU and increase the I/O throughput on multiprocessor systems with multiple I/O ports. No user application changes are needed to take advantage of Fast Path. Fast Path can be utilized by the \$QIO system service or the Fast I/O services.

Extended File Cache (XFC)

Extended File Cache (XFC) is a virtual block data cache. Similar to the Virtual I/O Cache, the XFC is a clusterwide, file system data cache. Both file system data caches are compatible and coexist in the OpenVMS Cluster. The XFC improves I/O performance with the following features that are not available with the virtual I/O cache:

- Read-ahead caching
- Automatic resizing of the cache
- Larger maximum cache size
- No limit on the number of closed files that can be cached
- Control over the maximum size of I/O that can be cached
- Control over whether cache memory is static or dynamic

Record Management Services (RMS)

RMS is a set of I/O services that helps application programs to process and manage files and records. Although it is intended to provide a comprehensive software interface to mass storage devices, RMS also supports device-independent access to unit-record devices. RMS supports sequential, relative, and indexed file organizations in fixed-length or variable-length record formats, and also supports byte stream formats for sequential file organization. RMS record access modes provide access to records in four ways:

- Sequentially
- Directly by key value
- Directly by relative record number
- Directly by record file address

RMS supports block I/O operations for performance-critical applications that require user-defined file organizations and record formats. RMS promotes safe and efficient file sharing by providing multiple file access modes and automatic record locking (where applicable). RMS offers the options of enabling global buffers for buffer sharing by multiple processes.

RMS utilities aid file creation and record maintenance. These utilities convert files from one organization and format to another; restructure indexed files for storage and access efficiency; and reclaim data structures within indexed files. These utilities also generate reports.

For systems that have DECnet or DECnet-Plus installed, RMS provides a subset of file and record management services to remote network nodes. Remote file operations are generally transparent to user programs.

Commands such as EDIT, CREATE, COPY, TYPE, and PRINT allow users to manipulate RMS records within RMS files at the DCL command level.

Disk and Tape Volumes

The system manager can organize disk volumes into volume sets. Volume sets can contain a mix of disk device types and can be extended by adding volumes. Within a volume set, files of any organization type can span multiple volumes. Files can be allocated to the set as a whole (the default) or to specific volumes within the set. Optionally, the system manager can allocate portions of indexed files to specific areas of a single disk or to specific volumes in a volume set. The system

Standard Features

manager can place quotas on a disk to control the amount of space individual users can allocate. Quota assignment is made by UIC and can be controlled for each individual volume set in the system (or for each individual volume if the volume is not part of a set).

The system manager can cache disk structure information in memory to reduce the I/O overhead required for file management services. Although not required to do so, users can preallocate space and control automatic allocation. For example, a file can be extended by a given number of blocks, contiguously or noncontiguously, for optimal file system performance.

The system applies software validity checks and checksums to critical disk structure information. If a disk is improperly dismounted because of user error or system failure, the system rebuilds the disk's structure information automatically the next time the disk is mounted. The system detects bad blocks and prevents their reuse once the files to which the blocks were allocated are deleted. On DIGITAL Storage Architecture (DSA) disks, the disk controller detects and replaces bad blocks automatically.

The system provides 255 levels of named directories and subdirectories whose contents are alphabetically ordered. Device and file specifications follow VSI conventions. Users can use logical names to abbreviate the specifications and to make application programs device and file name independent. Users can assign a logical name to an entire specification, to a portion of a specification, or to another logical name.

OpenVMS supports multivolume magnetic tape files with transparent volume switching. Access positioning is done either by file name or by relative file position.

Application Modernization and Integration Technologies

Application Modernization and Integration Infrastructure products provide Internet, e-business, and integration software technologies that enable the development of e-business and enterprise integration solutions. These technologies are bundled with OpenVMS. Several of the components are additionally bound by an open source software license.

The following components are included in the Base Operating Environment (BOE) for OpenVMS for Integrity servers:

- VSI Secure Web Server (SWS)
- Universal Description, Discovery, and Integration (UDDI) Client Toolkit
- Web Services Integration Toolkit (WSIT)

Additional information can be found in the documentation contained in each product's software kit.

Associated Products

The products in this section are not licensed as part of the OpenVMS Operating System and require a separate license.

VSI OpenVMS Cluster Software

VSI OpenVMS Cluster software is available, both as a separately licensed layered product and within the High Availability Operating Environment (HA-OE) package. It provides a highly integrated OpenVMS computing environment that is distributed over multiple systems, separated in distance measured from feet up to 500 miles, containing up to 96 nodes.

OpenVMS Cluster systems and storage communicate using a combination of the following interconnects:

- Ethernet
- Small Computer Systems Interface (SCSI) (Storage Only)
- Fibre Channel (Storage Only)

VSI TCP/IP Services (minimum Version 5.7-13ECO05B) is needed if using IP for cluster communication. For more information, see the *Guidelines for OpenVMS Cluster Configurations and OpenVMS Cluster Systems* guides.

Applications running on one or more nodes in an OpenVMS Cluster system share resources in a coordinated manner.

Standard Features

While updating data, the OpenVMS Cluster software synchronizes access to shared resources, preventing multiple processes on any node in the cluster from uncoordinated access to shared data. This coordination ensures data integrity during concurrent update transactions.

Mixed-architecture and mixed-version clusters that contain both Alpha systems and Integrity server systems are supported. Cluster satellite boot support on Integrity server systems provides support for Integrity-to-Integrity satellite booting. Cross-architecture booting (booting an Integrity satellite node from an Alpha boot server and vice-versa) is not supported. For more information, see the *VSI OpenVMS Cluster Software Product Description* (SPD DO-VIBHAA-033).

VSI Volume Shadowing for OpenVMS

VSI Volume Shadowing for OpenVMS performs disk mirroring operations using a redundant array of independent disks (RAID-1) storage strategy. Volume Shadowing for OpenVMS is available as a separately licensed product, as well as a component of the High Availability Operating Environment (HA-OE). Volume Shadowing provides high data availability for disk devices by ensuring against data loss that results from media deterioration or controller or device failure. This prevents storage subsystem component failures from interrupting system or application tasks. For more information, see the *VSI Volume Shadowing for OpenVMS Software Product Description* (SPD DO-VIBHAA-031).

VSI RMS Journaling for OpenVMS

VSI RMS Journaling for OpenVMS is available as layered products and as a part of the High Availability Operating Environment (HA-OE) on Integrity servers. Journaling enables a system manager, user, or application to maintain the data integrity of RMS files in the event of a number of failure scenarios. These journaling products protect RMS file data from becoming lost or inconsistent.

RMS Journaling provides the following three types of journaling:

- After-image journaling. Allows users to reapply modifications that have been made to a file. This type of journaling allows users to recover files that are inadvertently deleted, lost, or corrupted.
- Before-image journaling. Allows users to reverse modifications that have been made to a file. This type of journaling allows users to return a file to a previously known state.
- Recovery-unit journaling. Allows users to maintain transaction integrity. A transaction can be defined as a series of file updates on one or more files. If any failure occurs during the transaction, recovery-unit journaling rolls back the partially completed transaction to its starting point.

The binary kit for RMS Journaling ships with the OpenVMS distribution kits. To run the software, customers must purchase a license and documentation. For more information, see the *VSI RMS Journaling for OpenVMS Software Product Description* (SPD DO-VIBHAA-030).

VSI TCP/IP Services for OpenVMS

VSI TCP/IP Services for OpenVMS is a System Integrated Product (SIP) that is licensed as part of the Base Operating Environment (BOE); a separate license is not required.

VSI TCP/IP Services is VSI's industry-standard implementation of the TCP/IP and NFS networking protocols on the OpenVMS platform; it is integrated with the OpenVMS operating system installation. VSI TCP/IP Services provides interoperability and resource sharing among systems running OpenVMS, UNIX, Windows, and other operating systems that support TCP/IP. TCP/IP provides a comprehensive suite of functions and applications that support industry-standard protocols for heterogeneous network communications and resource sharing. VSI TCP/IP Services provides a full TCP/IP protocol suite including IP/multicasting, dynamic load balancing, rlogin proxy, network file access, remote terminal access, remote command execution, remote printing, mail, application development, Post Office Protocol (POP), SNMP Extensible agent (eSNMP), and Finger Utility. TCP/IP Version 5.7 also enables packet processing Engine (PPE), FTP anonymous light and stream control transmission protocol (SCTP) for its customers.

Refer to the *VSI TCP/IP Services for OpenVMS Software Product Description* (SPD DO-VIBHAA-029) for further information.

Standard Features

VSI DECnet-Plus and VSI DECnet Software

VSI DECnet for Integrity server software is a System Integrated Product (SIP). DECnet for OpenVMS for Integrity servers is a component of the Base Operating Environment (BOE) on Integrity servers license bundle.

The license for DECnet for OpenVMS for Integrity servers also grants the rights to use DECnet-Plus. Note that only one version of DECnet can be active on a single system at any one time. Both DECnet and DECnet-Plus allow OpenVMS systems to participate in network task-to-task communications for the purposes of transfer and copy of files, printing, the running of applications, etc.

DECnet-Plus offers task-to-task communications, file management, downline system and task loading, network command terminals, and network resource sharing capabilities as defined in the DIGITAL Network Architecture (DNA) Phase V protocols. DECnet-Plus provides the newest DECnet features such as extended addressing and downline-load performance enhancements. DECnet-Plus integrates DECnet and OSI protocols and now provides a linkage to TCP/IP using Request for Comments (RFC) 1006 and RFC 1859. DECnet and OSI applications can now be run over DECnet (NSP), OSI (CLNS), and TCP/IP transports. For more information, see the Associated Products section of this QuickSpec.

For further information, see the *VSI DECnet-Plus for OpenVMS Software Product Description* (SPD DO-VIBHAA-023), or the *VSI DECnet for OpenVMS Software Product Description* (SPD DO-VIBHAA-024).

VSI DECram for OpenVMS

VSI DECram for OpenVMS is a disk device driver that improves I/O performance by allowing an OpenVMS system manager to create pseudo disks (RAMdisks) that reside in main memory. Frequently accessed data can be accessed much faster from a DECram device than from a physical disk device. These RAMdisks can be accessed through the file system just as physical disks are accessed, requiring no change to application or system software.

Because main memory is allocated for the DECram device, extra memory is generally required. The OpenVMS system manager can designate the amount of memory dedicated to the DECram devices and the files that will be stored on it. To run the DECram software, customers must first purchase a separate license.

For VSI OpenVMS for Integrity server customers, a software license for VSI DECram may be purchased as part of the OpenVMS Base Operating Environment (BOE).

For more information, refer to the *VSI DECram for OpenVMS Software Product Description* (SPD DO-VIBHAB-005).

VSI DECwindows Motif for OpenVMS

VSI DECwindows Motif for OpenVMS is a System Integrated Product (SIP). On the Integrity Server platform, the DECwindows product is part of the Base Operating Environment (BOE) and is licensed under this package.

This product provides support for both OSF/Motif, a standards-based graphical user interface, and the X user interface (XUI) in a single, run-time and development environment. DECwindows Motif displays the OSF/Motif user interface. Because both Motif and XUI are based on X.org X Window System, applications written with either toolkit will run regardless of which environment the user selects.

For more information, see the *VSI DECwindows Motif for OpenVMS Software Product Description* (SPD DO-VIBHAA-026).

Standard Features

Distributed Computing Environment (DCE) Support

The DCE for the OpenVMS product family provides a set of the distributed computing features specified by The Open Group's DCE, as well as tools for application developers. With DCE, The Open Group has established a standard set of services and interfaces that facilitate the creation, use, and maintenance of client/server applications.

DCE for OpenVMS serves as the basis for an open computing environment where networks of multivendor systems appear as a single system to the user. Because DCE makes the underlying networks and operating systems transparent, application developers can easily build portable, interoperable client/server applications. Users can locate and share information safely and easily across the entire enterprise. DCE for OpenVMS supplies system managers with a set of tools to consistently manage the entire distributed computing environment, while assuring the integrity of the enterprise.

DCE for OpenVMS consists of the following products:

- DCE Run-Time Services for OpenVMS
- DCE Application Developers' Kit for OpenVMS
- DCE Cell Directory Service (CDS)
- DCE Security Server, one of which is required for each DCE

The right to use the DCE Run-Time Services is included with the OpenVMS operating system base license. All other DCE products are available as separate layered products. For more details, see the *VSI Distributed Computing Environment (DCE) for OpenVMS Software Product Description* (SPD DO-VIBHAA-027).

Support for OSF/Motif and X Window System Standards

DECwindows Motif provides support for OSF/Motif, a standards-based graphical user interface. DECwindows Motif also provides support for the X Consortium's X Window System, Version 11, Release 6 (X11R6) server and the Version 11, Release 5 (X11R5) client.

Standard Features

Standards Supported by OpenVMS

The OpenVMS operating system is based on the following public, national, and international standards that are developed by the American National Standards Institute (ANSI), U.S. Federal Government (responsible for FIPS), Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO). The following information may be useful in determining responsiveness to stated conformance requirements as enabled in particular commercial and/or government procurement solicitation documents.

- ANSI X3.4-1986: American Standard Code for Information Interchange
- ANSI X3.22-1973: Recorded Magnetic Tape (800 BPI, NRZI)
- ANSI X3.27-1987: File Structure and Labeling of Magnetic Tapes for Information Interchange
- ANSI X3.298: Limited support. Information Technology—AT Attachment-3 Interface (ATA-3)
- ANSI X3.39-1986: Recorded Magnetic Tape (1600 BPI, PE)
- ANSI X3.40-1983: Unrecorded Magnetic Tape
- ANSI X3.41-1974: Code Extension Techniques for Use with 7-bit ASCII
- ANSI X3.42-1975: Representation of Numeric Values in Character Strings
- ANSI X3.54-1986: Recorded Magnetic Tape (6250 BPI, GCR)
- ANSI X3.131-1986 (SCSI I): Small Computer System Interface
- ANSI X3.131-1994 (SCSI II): Small Computer System Interface
- ANSI/IEEE 802.2-1985: Logical Link Control
- ANSI/IEEE 802.3-1985: Carrier Sense Multiple Access with Collision Detection
- FIPS 1-2: Code for Information Interchange, Its Representations, Subsets, and Extensions
NOTE: 1-2 includes ANSI X3.4-1977(86)/FIPS 15; ANSI X3.32-1973/FIPS 36; ANSI X3.41-1974/FIPS 35; and FIPS 7.
- FIPS 3-1/ANSI X3.22-1973: Recorded Magnetic Tape Information Interchange (800 CPI, NRZI)
- FIPS 16-1/ANSI X3.15-1976: Bit Sequencing of the Code for Information Interchange in Serial-by-Bit Data Transmission
Note: FED STD 1010 adopts FIPS 16-1.
- FIPS 22-1/ANSI X3.1-1976: Synchronous Signaling Rates Between Data Terminal and Data Communication Equipment
Note: FED STD 1013 adopts FIPS 22-1.
- FIPS 25/ANSI X3.39-1986: Recorded Magnetic Tape for Information Interchange (1600 CPI, Phase Encoded)
- FIPS 37/ANSI X3.36-1975: Synchronous High-Speed Data Signaling Rates Between Data Terminal Equipment and Data Communication Equipment
NOTE: FED STD 1001 adopts FIPS 37.
- FIPS 50/ANSI X3.54-1986: Recorded Magnetic Tape for Information Interchange, 6250 CPI (246 CPMM), Group Coded Recording
- FIPS 79/ANSI X3.27-1987: Magnetic Tape Labels and File Structure for Information Interchange
- FIPS 86/ANSI X3.64-1979: Additional Controls for Use with American National Standard Code for Information Interchange
NOTE: Other FIPS are not applicable.
NOTE: Information regarding interchangeability of ANSI and FED standards with FIPS is contained in "ADP Telecommunications Standards Index," July 1988, published and maintained by the General Services Administration.
- ISO 646: ISO 7-bit Coded Character Set for Information Exchange
- ISO 1001: File Structure and Labeling of Magnetic Tapes for Information Interchange
- ISO 1863: Information Processing — 9-track, 12, 7 mm (0.5 in) wide magnetic tape for information interchange recorded at 32 rpm (800 rpi)
- ISO 1864: Information Processing—Unrecorded 12, 7 mm (0.5 in) wide magnetic tape for information interchange — 35 ft/mm (800 ft/pi) NRZI, 126 ft/mm (3 200 ft/pi) phase encoded and 356 ft/mm (9 042 ft/pi), NRZI
- ISO 2022: Code Extension Techniques for Use with ISO 646
- ISO 3307: Representations of Time of the Day
- ISO 3788: Information Processing — 9-track, 12, 7 mm (0.5 in) wide magnetic tape for information interchange recorded at 63 rpm (1 600 rpt), phase encoded
- ISO 4873: 8-Bit Code for Information Interchange — Structure and Rules for Implementation
- ISO 5652: Recorded Magtape (6250)
- ISO 6429: Control Functions for Coded Character Sets
- ISO 9316: 1989 (SCSI-1) Small Computer System Interface
- ISO 9660: Information Processing—Volume and file structure of CD-ROM for information exchange
- ISO 10288: 1994 (SCSI-2) Small Computer System Interface

Technical Specifications

Installation

OpenVMS for Integrity servers is distributed as a binary kit on DVD. Procedures for setting up the system disk from media and for preparing the system for day-to-day operations are provided in the *VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual*. The procedures use the POLYCENTER Software Installation (PCSI) utility to configure and install the OpenVMS Integrity operating system.

Network Installation and Upgrade

InfoServer network booting is supported for OpenVMS installations and upgrades on any OpenVMS Integrity server systems that support OpenVMS. For OpenVMS Integrity server systems, InfoServer network booting is supported on all LAN cards (also referred to as LAN devices or adapters) that are supported by EFI.

For OpenVMS Integrity server installations and upgrades, you can boot from a virtual DVD/CD drive on the LAN using the OpenVMS InfoServer software application. You can use the OpenVMS InfoServer software application on all OpenVMS Integrity server systems running Version 8.3 or higher. This support provides the additional advantage of allowing a network administrator to boot multiple OpenVMS systems on the network from a single copy of the OpenVMS distribution CD or DVD.

Using the InfoServer software application on Integrity servers for network booting requires several one-time-only configuration steps unique to OpenVMS Integrity servers. Any configuration procedures that might have been performed for network booting using an InfoServer hardware system (traditionally used by Alpha systems) are not valid for the OpenVMS Integrity servers. Booting from the InfoServer software application for OpenVMS on Integrity servers differs significantly from booting from the InfoServer hardware system traditionally used by OpenVMS Alpha systems or from the InfoServer software application on OpenVMS Alpha systems.

To install or upgrade the operating system over the network, OpenVMS Integrity server systems must use the InfoServer software application that is integrated with the OpenVMS operating system.

For additional information, see the *VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual*.

Virtual Connect

Virtual Connect is a set of interconnect modules and embedded software for HPE BladeSystem c-Class enclosures; it simplifies the setup and administration of server connections.

Virtual Media (vMedia)

Virtual Media (vMedia) is the overall name for a number of different devices that can exist on a PC. These devices appear as local USB disk devices to the host system. You can also use vMedia devices to boot, install, or upgrade OpenVMS from over the network, as described in the *VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual*.

VSI OpenVMS V8.4-2L1 supports vMedia in the following Integrity server systems: BL860c i2, BL860c i4, BL870c i2, BL870c i4, BL890c i2, BL890c i4, rx2800 i2, and rx2800 i4.

POLYCENTER Software Installation

The PCSI utility simplifies the installation and management of OpenVMS products. It is used to install, update, and uninstall software products that have been prepared with the utility. In addition, the utility provides a database to track the installation, reconfiguration, and uninstallation of software. For products installed with other installation technologies, the utility provides a mechanism for adding information about them into the product database. The utility also provides the ability to manage dependencies between products during the installation process.

Technical Specifications

For software providers, the PCSI utility simplifies the task of packaging software by providing a simple, declarative language for describing material for the installation kit and defining how it is installed. The utility handles the functions, while the developer instructs the utility what to do. This significantly reduces the complexity and time to develop installation procedures. The language allows the developer to easily specify dependencies on other software, manage objects in the execution environment (such as files and directories), and anticipate and resolve conflict before it occurs. The utility also significantly simplifies the packaging of multiple software products into one logical product suite.

For OpenVMS for Integrity servers, you use the PCSI utility to install the operating system and to install layered products that are compliant with the POLYCENTER utility.

All of the software product kits included on the OpenVMS Version 8.4-2L1 distribution media are signed using Secure Delivery. A notable exception is the OpenVMS Operating System (the VMS product) because it is shipped in bootable form, not as a single file kit that is signed.

For OpenVMS for Integrity servers, when you install or upgrade the operating system by booting from the distribution media, layered products that have been signed are validated by the PCSI utility with the aid of a digital signature file (called a manifest). Validation involves using the Secure Delivery component of CDSA to authenticate the originator of the product kit and to verify its contents.

In addition, on OpenVMS for Integrity server systems, the PRODUCT SHOW HISTORY command displays the validation status of installed products and identifies those that were installed from unsigned kits or were installed prior to the availability of the Secure Delivery functionality.

VMSINSTAL

OpenVMS includes the VMSINSTAL facility to handle the installation of optional VSI supplied software products that have not been converted to use the POLYCENTER Software Installation utility.

Test Package and Diagnostics

OpenVMS includes a User Environment Test Package (UETP), which verifies that the OpenVMS operating system is properly installed and ready for use on the customer's systems. You can run diagnostics on individual devices during normal system operation. Certain critical components can operate in degraded mode.

OpenVMS For Integrity Servers Disk Space Requirements

Operating System Disk Space Requirements

The minimum disk space required for OpenVMS for Integrity servers is 3.4 GB. The disk space requirements for OpenVMS for Integrity servers vary according to which options are installed:

File Category	Space Used
Minimum OpenVMS files	2.4 GB
DECwindows Support	74 MB
Full DECwindows Motif (optional)	132 MB
DECnet Support	3 MB
DECnet-Plus	66 MB
WBEMCIM	308 MB
Other optional OpenVMS files	167 MB
Paging file (required)	1028 MB
Swap file (suggested)	32 MB
Dump file (optional)	181 MB
Total	3.4 GB

Technical Specifications

NOTE: The minimum OpenVMS files listed in the table will allow you to run with minimal functionality. Not all OpenVMS commands and utilities will function fully as documented in this minimum configuration. Not all VSI and other layered products will work in this minimum configuration.

The minimum OpenVMS files are for a system configuration where all optional features have been declined during the initial installation. For most applications, this is not a realistic OpenVMS environment.

The paging, swap, and dump file requirements are the minimum for a system with 64 MB of main memory. Additional memory in most cases adds to the space needed for these files, as will particular needs of your application. With careful system management it is possible to use the paging file space as a temporary dump file.

For an OpenVMS Cluster system disk, paging, swap, and dump files cannot be shared between nodes, so the files must either be duplicated on the system disk or located on some other disk.

DECwindows Motif for OpenVMS for Integrity servers Disk Space Requirements

To support full OpenVMS for Integrity servers and full DECwindows Motif for OpenVMS for Integrity servers, a system disk with at least 707 MB is recommended. However, a subset of the DECwindows Motif environment can be installed. The permanent amount of space used is 135 MB. These disk space requirements are in addition to the disk space required for the OpenVMS for Integrity servers operating system, as indicated in the OpenVMS for Integrity servers Disk Space Requirements table.

Installation of the DECwindows Motif layered product gives customers the option of installing any or all of the following components:

- Run-time support (base kit) – 60 MB. This section provides support for running DECwindows Motif for OpenVMS for Integrity servers applications on Integrity servers and is a required part of the installation.
- New Desktop – 35 MB. This is an optional component that allows use of the New Desktop environment. It includes applications and application programming interfaces (APIs).
- DECwindows desktop – 8 MB. The DECwindows desktop is the user interface that was included in previous versions of DECwindows Motif and includes the DECwindows Session Manager, FileView, and the Motif Window Manager.
- Programming support – 8 MB. This number includes support for the C, Pascal, and Fortran programming languages and for the New Desktop. If only a subset of languages is installed, the amount of disk space required will be less.
- Programming examples – 8 MB. This number includes example audio files, the DECwindows desktop, and the New Desktop. If only a subset of example files is installed, the amount of disk space required will be less.

Layered Product Disk Space Requirements

In addition to the disk space used directly by VSI or third-party layered products, there may be additional space used to store information from those products in OpenVMS help libraries, command tables, object libraries, and elsewhere. The amount of additional disk space required cannot be exactly predicted due to the possibility of recovering unused space already existing in those library files. Unusually large modules contributed by layered products can also affect the amount of space required for upgrading to a new version of the OpenVMS for Integrity servers operating systems.

Technical Specifications

Distribution Media

OpenVMS for Integrity servers

OpenVMS for Integrity servers is available on DVD. The OpenVMS for Integrity servers binary DVD contains the operating system and layered product binaries for all layered products included with the Operating Environments. Other items in the OpenVMS for Integrity Servers kit are delivered on CD or DVD. A single media kit contains the operating system, Operating Environment component products, layered products, online documentation, and several hardcopy manuals.

Some Integrity servers do not include a built-in CD/DVD drive. You can use an external USB CD/DVD drive (you must supply this drive and the required cable; they are not included with the Integrity servers). You can use InfoServer network booting to boot from a virtual DVD drive on the network. In addition, beginning with OpenVMS Version 8.4, you can use HPE SIM provisioning for similar purposes, in which case you can install or upgrade OpenVMS on multiple servers (up to 8) in the network simultaneously. You can also use virtual media (vMedia) devices to allow you to boot, install, or upgrade OpenVMS from over the network, as described in the *VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual*.

Documentation

For OpenVMS Version 8.4-2L1, documentation is available in the following formats:

Printed Books

For OpenVMS Version 8.4-2L1, the following hardcopy books are included in the media kit. These books are also available on the VMS Software Inc website, and on the VSI OpenVMS OE DVD:

- VSI OpenVMS Version 8.4-2L1 Cover Letter and Release Notes
- VSI OpenVMS Version 8.4-2 Cover Letter and Release Notes
- VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual
- VSI OpenVMS Version License Management Utility Manual

Online Books

The OpenVMS Version 8.4-2L1 for Integrity servers media kit contains an online documentation CD for the Operating Environment.

Growth Considerations

The minimum hardware and software requirements for any future version of this product may be different from the requirements for the current version.

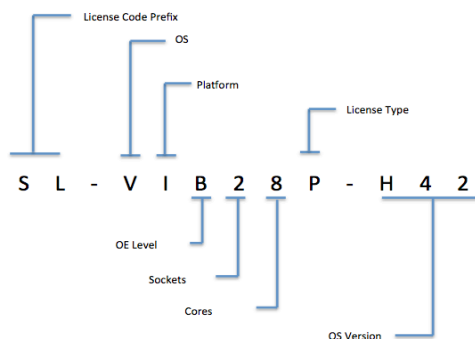
OpenVMS for Integrity Servers Ordering Information

VSI OpenVMS V8.4-2L1 is sold by the socket, and is sold and supported on the systems listed on page 2. VSI utilizes a 2-6-3 part number format, where the first 2 numbers represent the product type:

SL = Software License	SV = Services (installation, data migration, etc.)
SW = Software Warranty	ME = Media
SA = Software Warranty Agreement	DO = Documentation
SK = Software Distribution Kit	TR = Education Courses and Training
HW = Hardware	

Technical Specifications

The following example illustrates the fields that comprise a Software License (SL) part number.



For licenses, the middle 6 fields denote the OS, platform, OS level, server sockets, socket cores, and license type:

- 1st position: V=OpenVMS
- 2nd position: Platform; I=Integrity
- 3rd position: OS level; B=BOE; H=HAOE
- 4th position: Sockets in server: 2=2 sockets, 4=4 sockets, 8=8 sockets, 1=16 sockets, 3=32 sockets
- 5th position: Cores per socket; 1=1 core, 2=2 core, 4=4 cores, 8=8 cores
- 6th position: License type: E=Electronic, P=Physical, T=Trade-in allowance, U=Upgrade

Last, a 3-letter code represents the OpenVMS version, minor update number, and hardware update number.

The OpenVMS Version 8.4-2L1 operating system software, layered product software, and online documentation are delivered together in one media kit.

- Specify part number **SK-VIHKIT-H4W** for the **VSI OpenVMS V8.4-2L1 Integrity servers OE media kit**.
- A single media kit provides the Base (BOE) and High Availability (HA-OE) Operating Environments, which are enabled by a BOE or HA-OE license-to-use (LTU, sold separately).
- Purchase of an OE media kit requires the purchase of a corresponding OE license on the same order.

For a complete description of the OpenVMS for Integrity servers Operating Environments, or for additional ordering information, see the *VSI OpenVMS Operating Environment for OpenVMS Integrity Servers Software Product Description* (SPD DO-VIBHA*-006).

OpenVMS for Integrity Servers Software Licenses

The following licenses are offered for each OpenVMS for Integrity servers Operating Environment. One license is required for each active socket.

Technical Specifications

Software Licenses

Table 1: Operating Environment Licenses with Options

VSI OpenVMS V842L1 Base Operating Environment LTU

Product Number	Description
SL-VIB21P-H4W	VSI V842L1 BOE 2S/1C LTU (physical license)
SL-VIB22P-H4W	VSI V842L1 BOE 2S/2C LTU (physical license)
SL-VIB24P-H4W	VSI V842L1 BOE 2S/4C LTU (physical license)
SL-VIB28P-H4W	VSI V842L1 BOE 2S/8C LTU (physical license)
SL-VIB41P-H4W	VSI V842L1 BOE 4S/1C LTU (physical license)
SL-VIB42P-H4W	VSI V842L1 BOE 4S/2C LTU (physical license)
SL-VIB44P-H4W	VSI V842L1 BOE 4S/4C LTU (physical license)
SL-VIB48P-H4W	VSI V842L1 BOE 4S/8C LTU (physical license)
SL-VIB81P-H4W	VSI V842L1 BOE 8S/1C LTU (physical license)
SL-VIB82P-H4W	VSI V842L1 BOE 8S/2C LTU (physical license)
SL-VIB84P-H4W	VSI V842L1 BOE 8S/4C LTU (physical license)
SL-VIB88P-H4W	VSI V842L1 BOE 8S/8C LTU (physical license)
SL-VIB21E-H4W	VSI V842L1 BOE 2S/1C E-LTU (electronic license)
SL-VIB22E-H4W	VSI V842L1 BOE 2S/2C E-LTU (electronic license)
SL-VIB24E-H4W	VSI V842L1 BOE 2S/4C E-LTU (electronic license)
SL-VIB28E-H4W	VSI V842L1 BOE 2S/8C E-LTU (electronic license)
SL-VIB41E-H4W	VSI V842L1 BOE 4S/1C E-LTU (electronic license)
SL-VIB42E-H4W	VSI V842L1 BOE 4S/2C E-LTU (electronic license)
SL-VIB44E-H4W	VSI V842L1 BOE 4S/4C E-LTU (electronic license)
SL-VIB48E-H4W	VSI V842L1 BOE 4S/8C E-LTU (electronic license)
SL-VIB81E-H4W	VSI V842L1 BOE 8S/1C E-LTU (electronic license)
SL-VIB82E-H4W	VSI V842L1 BOE 8S/2C E-LTU (electronic license)
SL-VIB84E-H4W	VSI V842L1 BOE 8S/4C E-LTU (electronic license)
SL-VIB88E-H4W	VSI V842L1 BOE 8S/8C E-LTU (electronic license)

Technical Specifications

VSI V842L1 HA-OE Environment LTU

SL-VIH21P-H4W	VSI V842L1 HAOE 2S/1C LTU (physical license)
SL-VIH22P-H4W	VSI V842L1 HAOE 2S/2C LTU (physical license)
SL-VIH24P-H4W	VSI V842L1 HAOE 2S/4C LTU (physical license)
SL-VIH28P-H4W	VSI V842L1 HAOE 2S/8C LTU (physical license)
SL-VIH41P-H4W	VSI V842L1 HAOE 4S/1C LTU (physical license)
SL-VIH42P-H4W	VSI V842L1 HAOE 4S/2C LTU (physical license)
SL-VIH44P-H4W	VSI V842L1 HAOE 4S/4C LTU (physical license)
SL-VIH48P-H4W	VSI V842L1 HAOE 4S/8C LTU (physical license)
SL-VIH81P-H4W	VSI V842L1 HAOE 8S/1C LTU (physical license)
SL-VIH82P-H4W	VSI V842L1 HAOE 8S/2C LTU (physical license)
SL-VIH84P-H4W	VSI V842L1 HAOE 8S/4C LTU (physical license)
SL-VIH88P-H4W	VSI V842L1 HAOE 8S/8C LTU (physical license)
SL-VIH21E-H4W	VSI V842L1 HAOE 2S/1C E-LTU (electronic license)
SL-VIH22E-H4W	VSI V842L1 HAOE 2S/2C E-LTU (electronic license)
SL-VIH24E-H4W	VSI V842L1 HAOE 2S/4C E-LTU (electronic license)
SL-VIH28E-H4W	VSI V842L1 HAOE 2S/8C E-LTU (electronic license)
SL-VIH41E-H4W	VSI V842L1 HAOE 4S/1C E-LTU (electronic license)
SL-VIH42E-H4W	VSI V842L1 HAOE 4S/2C E-LTU (electronic license)
SL-VIH44E-H4W	VSI V842L1 HAOE 4S/4C E-LTU (electronic license)
SL-VIH48E-H4W	VSI V842L1 HAOE 4S/8C E-LTU (electronic license)
SL-VIH81E-H4W	VSI V842L1 HAOE 8S/1C E-LTU (electronic license)
SL-VIH82E-H4W	VSI V842L1 HAOE 8S/2C E-LTU (electronic license)
SL-VIH84E-H4W	VSI V842L1 HAOE 8S/4C E-LTU (electronic license)
SL-VIH88E-H4W	VSI V842L1 HAOE 8S/8C E-LTU (electronic license)

Technical Specifications

Ordering OE License Upgrades

The Upgrade License is used when the Operating Environment is upgraded from a smaller OE to larger OE on the same Integrity server. The BOE to HA-OE License Upgrades deliver a license for HA-OE and the pricing gives credit for the previous purchase of the BOE. Table 2 lists the OE license upgrade options.

Table 2

OE License Upgrade Options

Product No.	Common Description
	VSI OpenVMS V842L1 Integrity servers BOE to HA-OE Upgrade
SL-VIH21U-H4W	VSI V842L1 BOE to HAOE Upg 2S/1C LTU
SL-VIH22U-H4W	VSI V842L1 BOE to HAOE Upg 2S/2C LTU
SL-VIH24U-H4W	VSI V842L1 BOE to HAOE Upg 2S/4C LTU
SL-VIH28U-H4W	VSI V842L1 BOE to HAOE Upg 2S/8C LTU
SL-VIH41U-H4W	VSI V842L1 BOE to HAOE Upg 4S/1C LTU
SL-VIH42U-H4W	VSI V842L1 BOE to HAOE Upg 4S/2C LTU
SL-VIH44U-H4W	VSI V842L1 BOE to HAOE Upg 4S/4C LTU
SL-VIH48U-H4W	VSI V842L1 BOE to HAOE Upg 4S/8C LTU
SL-VIH81U-H4W	VSI V842L1 BOE to HAOE Upg 8S/1C LTU
SL-VIH82U-H4W	VSI V842L1 BOE to HAOE Upg 8S/2C LTU
SL-VIH84U-H4W	VSI V842L1 BOE to HAOE Upg 8S/4C LTU
SL-VIH88U-H4W	VSI V842L1 BOE to HAOE Upg 8S/8C LTU

Technical Specifications

Ordering OE License Trade-ins

VSI trade-in policy provides software investment protection when the customer is moving to a new Integrity server. To be eligible for credit, the user needs a valid license. The old software must be equivalent in function to the new software. The trade-in credit is 50% of the purchase price of the target license. NOTE: VSI supports trade-ins from Alpha and VAX.

Trade-in Policy Example: HPE Alpha to VSI OpenVMS Operating Environment

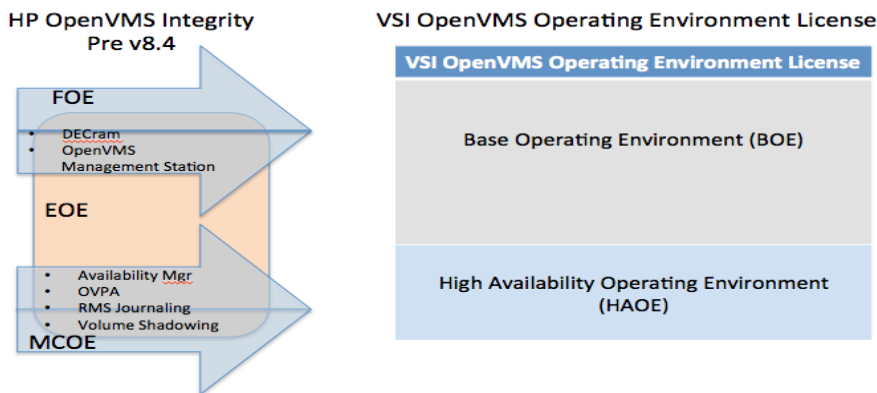
HP OpenVMS Alpha	VSI OpenVMS Operating Environment License
OpenVMS Base	Base Operating Environment (BOE)
OpenVMS SMP	
OpenVMS User	
Enterprise Integration Package	
DECram	High Availability Operating Environment (HAOE)
RMS Journaling	
Volume Shadowing	
VMSClusters	

Example 1: Trade-in Base, 3 SMPs, Users and EIP from a four CPU server; receive credit for 4 BOE PSL licenses on the target server

Example 2: Trade-in all of the above plus 2 of the 3 HAOE products and receive credit for 4 BOE PSL licenses

Example 3: Trade-in all of the above plus VMSClusters and receive credit for 4 HAOE PSL licenses

Trade-in Policy Example: HPE OpenVMS Integrity Pre v8.4 to VSI OpenVMS Integrity Operating Environment



Trade-in equivalency for older OEs (FOE, EOE, MCOE):

FOE -> BOE

EOE -> HA-OE

MCOE -> HA-OE

Process:

1. The customer orders the new OE license.
2. The customer provides proof of license and proof of support to the field representative.
3. The field calculates credit and applies it to the order.
4. License keys for the old system should be deleted at least 90 days after the new licenses/new system delivery.

Technical Specifications

Table 3 lists the OE license trade-ins.

Table 3: OE License Trade-ins

Product Number	Description
VSI V842L1 BOE Trade-in LTU	
SL-VIB21T-H4W	VSI V842L1 BOE Trade-in 2S/1C LTU
SL-VIB22T-H4W	VSI V842L1 BOE Trade-in 2S/2C LTU
SL-VIB24T-H4W	VSI V842L1 BOE Trade-in 2S/4C LTU
SL-VIB28T-H4W	VSI V842L1 BOE Trade-in 2S/8C LTU
SL-VIB41T-H4W	VSI V842L1 BOE Trade-in 4S/1C LTU
SL-VIB42T-H4W	VSI V842L1 BOE Trade-in 4S/2C LTU
SL-VIB44T-H4W	VSI V842L1 BOE Trade-in 4S/4C LTU
SL-VIB48T-H4W	VSI V842L1 BOE Trade-in 4S/8C LTU
SL-VIB81T-H4W	VSI V842L1 BOE Trade-in 8S/1C LTU
SL-VIB82T-H4W	VSI V842L1 BOE Trade-in 8S/2C LTU
SL-VIB84T-H4W	VSI V842L1 BOE Trade-in 8S/4C LTU
SL-VIB88T-H4W	VSI V842L1 BOE Trade-in 8S/8C LTU
VSI V842L1 HAOE Trade-in LTU	
SL-VIH21T-H4W	VSI V842L1 HAOE Trade-in 2S/1C LTU
SL-VIH22T-H4W	VSI V842L1 HAOE Trade-in 2S/2C LTU
SL-VIH24T-H4W	VSI V842L1 HAOE Trade-in 2S/4C LTU
SL-VIH28T-H4W	VSI V842L1 HAOE Trade-in 2S/8C LTU
SL-VIH41T-H4W	VSI V842L1 HAOE Trade-in 4S/1C LTU
SL-VIH42T-H4W	VSI V842L1 HAOE Trade-in 4S/2C LTU
SL-VIH44T-H4W	VSI V842L1 HAOE Trade-in 4S/4C LTU
SL-VIH48T-H4W	VSI V842L1 HAOE Trade-in 4S/8C LTU
SL-VIH81T-H4W	VSI V842L1 HAOE Trade-in 8S/1C LTU
SL-VIH82T-H4W	VSI V842L1 HAOE Trade-in 8S/2C LTU
SL-VIH84T-H4W	VSI V842L1 HAOE Trade-in 8S/4C LTU
SL-VIH88T-H4W	VSI V842L1 HAOE Trade-in 8S/8C LTU

Technical Specifications

OpenVMS Hardcopy Documentation Sets

Hardcopy Documentation offerings are being phased out due to low demand. OpenVMS operating system and layered product documentation can be found on www.vmssoftware.com.

Software Licensing

OpenVMS operating system software is furnished under the licensing provisions of VSI's Standard Terms and Conditions.

License Management Facility Support

The OpenVMS operating system supports the OpenVMS License Management Facility (LMF). If an OpenVMS license is not registered and activated using LMF, only a single login is permitted for system management purposes through the system console (OPA0:).

Some of the OpenVMS license types are based on the number of concurrent users, called an activity license. Every product has the option to define an activity as related to the LMF. OpenVMS Interactive User and ADL Interactive User Licenses define the number of concurrent users who have activity licenses as defined by the LMF.

OpenVMS defines activities, sometimes referred to as an OpenVMS user, as follows:

- Each remote terminal connection is considered an activity. This is true even if users set host to their local nodes (SET HOST 0).
- Each connection from a terminal server is considered an activity.
- A multiple window session on a workstation is considered one activity, regardless of the number of windows.
- A batch job is not considered an activity.
- A remote network connection (a connection other than a remote terminal connection) is not considered an activity.

For more information about VSI's licensing terms and policies, contact your VSI account representative.

Software License Information (OpenVMS for Integrity Servers Only)

OpenVMS is offered with Per Socket License (PSL) on HPE Integrity server Blades (BL8x0c i2/i4 server blades and rx2800 i2/i4 servers).

The OE bundles are groups of individual products offered together under a single license. OEs are offered with PSLs. One PSL is required for each active processor socket in the system or hard partition. If additional processor sockets are later added to the system or hard partition, each requires an additional PSL.

An OE license grants the right to use all the components included in the specified OE.

For OpenVMS for Integrity servers, once a customer purchases a new license, the only way the customer can obtain rights to new versions of the product are:

- Through a VSI Support Agreement
- Through a purchase of a new, full priced, VSI license for that product

Other differences from OpenVMS Alpha licensing practices:

- User licenses are not required. The Base Operating Environment (BOE) license includes unlimited OpenVMS users.
- Version update licenses are not available. Update services are available only through a Support Agreement.
- Trade-in allowances are offered as license "options" rather than as separate licenses.

For more information regarding OpenVMS for Integrity servers licensing terms and policies, contact your local VSI sales office.

The following technologies are licensed as part of the OpenVMS for Integrity servers operating system:

Technical Specifications

Product Name

VSI DECprint Supervisor (DCPS) for OpenVMS
VSI Distributed Computing Environment (DCE)

Software Product Description (SPD)

SPD DO-VIBHAA-025
SPD DO-VIBHAA-027

Integrity Server Systems Supported

The following HPE Integrity servers are supported by VSI OpenVMS Version 8.4-2L1:

- HPE Integrity BL860c i2 Server Blade (Itanium Quadcore processors); 1.33GHz/16MB, 1.6GHz/20MB, 1.73GHz/24MB; included in c7000 and c3000 enclosure
- HPE Integrity BL860c i2 Server Blade (Itanium Dualcore processors); 1.6GHz/10MB; included in c7000 and c3000 enclosure
- HPE Integrity BL870c i2 Server Blade (Itanium Quadcore processors); 1.33GHz/16MB, 1.6GHz/20MB, 1.73GHz/24MB; included in c7000 and c3000 enclosure
- HPE Integrity BL870c i2 Server Blade (Itanium Dualcore processors); 1.6GHz/10MB; included in c7000 and c3000 enclosure
- HPE Integrity BL890c i2 Server Blade (Itanium Quadcore processors) 1.33GHz/16MB, 1.6GHz/20MB, 1.73GHz/24MB; included in c7000 and c3000 enclosure
- HPE Integrity BL890c i2 Server Blade (Itanium Dualcore processors); 1.6GHz/10MB; included in c7000 and c3000 enclosure
- HPE Integrity rx2800 i2 Server (Itanium Quad-core Processors); 1.33 GHz/16 MB on-chip L3 cache 9320 processor, or quad core 1.60 GHz/20 MB on-chip L3 cache 9340.
- HPE Integrity rx2800 i2 Server (Itanium Dual-core Processors); 1.6 GHz/10 MB on-chip L3 cache 9310 processor
- HPE Integrity BL860c i4 Server Blade (Itanium Quadcore processors); 1.73GHz/20MB 130W; 2.4GHz/32MB 170W included in c7000 and c3000 enclosure
- HPE Integrity BL860c i4 Server Blade (Itanium Dualcore processors); 2.13GHz/24MB 170W; 2.53GHz/32MB 170W; included in c7000 and c3000 enclosure
- HPE Integrity BL870c i4 Server Blade (Itanium Quadcore processors); 1.73GHz/20MB 130W; 4-Core 9550 2.4GHz/32MB 170W, 1.6GHz/20MB, 1.73GHz/24MB; included in c7000 and c3000 enclosure
- HPE Integrity BL870c i4 Server Blade (Itanium Dualcore processors); 2.13GHz/24MB 170W; 2.53GHz/32MB 170W; included in c7000 and c3000 enclosure
- HPE Integrity BL890c i4 Server Blade (Itanium Quadcore processors) 2.13GHz/24MB 170W; included in c7000 and c3000 enclosure
- HPE Integrity BL890c i4 Server Blade (Itanium Dualcore processors); 2.53GHz/32MB 170W; included in c7000 and c3000 enclosure
- HPE Integrity rx2800 i4 Server (Itanium Quad-core Processors); 1.73GHz/20MB 130W on-chip L3 cache 9520 processor, or quad core 2.4GHz/32MB 170W on-chip L3 cache 9550.
- HPE Integrity rx2800 i4 Server (Itanium Dual-core Processors); 2.13GHz/24MB 170W on-chip L3 cache 9540 or 2.53GHz/32MB 170W on 9560 processor
- HPE Integrity rx1600 Server (2P/2C); 1.0GHz
- HPE Integrity rx2600 Server (2P/2C); 1.5, 1.4, 1.3, 1.0 GHz
- HPE Integrity rx2620 Server (2P/4C); 1.6GHz/18MB 1.4GHz/12MB
- HPE Integrity rx2620 Server (2P/2C); 1.6GHz/6MB 1.6GHz/3MB (DP), 1.3GHz/3MB (DP)
- HPE Integrity rx2660 Server (2P/2C, 2P/4C); 1.6GHz/6MB, 1.4GHz/12MB, 1.6GHz/18MB
- HPE Integrity rx3600 Server (2P/4C); 1.6GHz/18MB, 1.4GHz/12MB
- HPE Integrity rx6600 Server (4P/8C); 1.6GHz/24MB, 1.6GHz/18MB, 1.4GHz/12MB
- HPE Integrity rx7640 Server, 2 cell (8P/16C); 1.6GHz/18MB, 1.4GHz/12MB
- HPE Integrity rx8640 Server, 4 cell (16P/32C); 1.6GHz/24MB, 1.6GHz/18MB, 1.4GHz/12MB

Appendix A (OpenVMS for Integrity servers)

This appendix describes the HPE options supported on HPE OpenVMS for HPE Integrity servers. It is left in this document for reference. Please refer to VSI's web page at www.vmssoftware.com for options supported by VSI's OpenVMS.

LAN Options

HPE PCI 10/100Base-T LAN Adapter (Linux Only)	A5230A
HPE 4-Port 100base-TX Ethernet LAN Adapter	A5506B
HPE GigE-TX PCI LAN Adapter (rx2600)	A6825A
HPE GigE-SX PCI LAN Adapter (rx2600)	A6847A
HPE PCI-X 2Port 1000Base-SX/T Gigabit Adapter	A7011A
HPE PCI-X 2-P SCSI/1000Base-T Multifunction Adapter	AB290A
HPE PCI-X 133MHz 10GbE SR Fiber Adapter	AB287A
HPE PCI-X 4-port 1000Base-T Adapter	AB545A
Dual port UTP (copper) network interface card (NIC) that connects PCI-X to Ethernet and IEEE 802.3 local area networks at 10, 100, or 1000 Mb/s. This card is supported as an rx4640 core I/O option only	AB352A
HPE PCI-X 1000Base-T Card	AD331A
HPE PCI-X 1-port 1000Base SX Adapter	AD332A
HPE PCIe 2-port 1000Base-T LAN Adapter	AD337A
HPE PCIe 2-port 1000Base-SX LAN Adapter	AD338A
HPE PCIe 4-port 1000Base-T Gigabit Adapter	AD339A
HPE PCI-X 266MHz 10Gb Ethernet SR Multi-OS Card	AD385A
NOTE: No boot support	
Quad port UTP (copper) network interface card (NIC); connects PCIe to Ethernet and IEEE 802.3 local area networks at 10, 100, or 1000 Mb/s.	NC364M
HPE NC360m Dual Port 1GbE BL-c Adapter	445978-B21
HPE NC364m Quad Port 1GbE BL-c Adapter	447883-B21
HPE NC532m Dual Port 10GbE Multifunction BL-c Adapter	467799-B21
HPE Integrity PCIe 2-port 10GbE-SR Fabric Adapter	AM225A
HPE Integrity PCIe 2-port 10GbE-LR Fabric Adapter	AM232A
HPE Integrity PCIe 2-port 10GbE-CR Copper Adapter	AM233A

Fibre Channel Storage Options

HPE PCI-X 2.0 Single-port 4GB FC Adapter	AB378B
HPE PCI-X 2.0 Dual-port 4GB FC Adapter	AB379B
HPE 4Gb 2-port PCIe Fibre Channel Host Bus Adapter	AD300A
HPE PCI Express 1-port 8Gb Fibre Channel SR (QLogic) Adapter	AH400A
HPE PCI Express 2-port 8Gb Fibre Channel SR (QLogic) Adapter	AH401A

Parallel SCSI Storage Options

HPE Smart Array 6402 U320 2CH Controller	A9890A
HPE Smart Array 6404 U320 4CH Controller	A9891A
HPE PCI-X Dual-Channel Ultra320 SCSI Adapter	A7173A
HPE Integrity PCI-E Ultra320 SCSI Adapter	AT134A

Serial Attached SCSI (SAS) Storage Options

HPE rx3600/rx6600 Core I/O Storage Controller	AB036B
HPE rx6600 2nd I/O Storage Controller	AB037B
HPE Integrity rx2660 SAS Smart Array P400 Card	AD397A
HPE Integrity rx3600/rx6600 Core I/O Upgrade	AD348A
HPE PCIe P800 SAS RAID Controller	AD335A
HPE PCIe SC44Ge SAS Host Bus Adapter	AH303A
HPE Smart Array P410/256 2-ports Int PCIe x8 SAS Controller.	462862- B21
HPE Smart Array P711m/1G 6Gb FBWC 4-ports Ext Mezzanine SAS Controller	513778-B21

Storage and Network Combo Cards

HPE PCI-X 2-P SCSI/1000Base-T Multifunction Adapter	AB290A
HPE PCI-X 2Gb FC/1Gb Ethernet Multifunction Adapter	AB465A

HPE 1000-SX and 2G FC PCI-X Combo Card	A9782A
HPE PCI-X 2G Fibre Channel/1000Base-T HBA	A9784A
HPE PCI-X 1-port 4Gb FC and 1-port 1000BT Adapter	AD193A
HPE PCI-X 2-port 4Gb FC and 2-port 1000BT Adapter	AD194A
HPE Server rx76xx/rp7420 Core I/O Card	A9918A
HPE PCIe 1-port 4Gb and 1-port 1000BT Adapter	AD221A
HPE PCIe 2-port 4Gb and 2-port 1000BT Adapter	AD222A

Tape Devices

320GB SDLT Tape Drive	SDLT320
600GB SDLT Tape Drive	SDLT600
400GB LTO Ultrium 2 Tape Drive	Ultrium 460
400GB LTO Ultrium 2 Tape Drive	Ultrium 448
400GB LTO Ultrium 2 Tape Blade	Ultrium 448c
800GB LTO Ultrium 3 Tape Drive	Ultrium 960
800GB LTO Ultrium 3 Tape drive	Ultrium 920
1.6TB LTO Ultrium 4 Tape Drive	Ultrium 1840
3TB LTO Ultrium 5 Tape Drive	Ultrium 3000
3TB LTO Ultrium 5 Tape Drive	Ultrium 3280
72GB DAT Tape Drive	DAT72
160GB DAT Tape Drive	DAT160
Tape Autoloader	1/8 Autoloader
Virtual Tape Library	VLS6000
Ultrium and SDLT Tape Library	MSL6000
Ultrium Tape Library	MSL2024
Ultrium Tape Library	MSL4048
Ultrium Tape Library	MSL8096
Ultrium and SDLT Tape Library	ESL E-Series
Ultrium Tape Library	EML E-Series

NOTE: Compressed capacity; assumes 2:1 data compression.

Parallel SCSI and SAS Storage Shelves

14 disk Ultra320 single-bus enclosure	MSA30 SB
14 disk Ultra320 double-bus enclosure	MSA30 DB
14 disk Ultra320 2-node Shared SCSI enclosure1	MSA30MI
12 3.5" SAS disk storage enclosure	MSA60
25 SFF SAS disk storage enclosure	MSA70
Half-height c-Class storage Blade with 6 SFF SAS disk	SB40c
HPE D2200sb PCIe Storage Blade	AP880A
SAS Storage System	MDS600
12 LFF 6Gb SAS/SATA disk enclosure	D2600
25 SFF 6Gb SAS/SATA disk enclosure	D2700
1Shelf is supported only on Integrity servers rx2620, rx2660, rx3600, rx6600.	

Miscellaneous Options

HPE USB OpenVMS Keyboard and 3-Button Mouse	AB552A
HPE Management (rx1600) CPU Card	A9803A
HPE OpenVMS/HPE-UX 2D/3D PCI Graphics Card	AB551A
HPE PCI-X iLO Remote Management Adapter	AD307A
HPE Graphics USB Card (rx5670)	A6869A
HPE Virtual Connect FlexFabric 10Gb/24-port Module for c-Class BladeSystem	571956-B21

Appendix B (OpenVMS for Integrity servers SAN Solutions)

This appendix describes the HPE storage options supported on HPE OpenVMS for HPE Integrity servers. It is left in this document for reference. Please refer to VSI's web page at www.vmssoftware.com for storage options supported by VSI's OpenVMS.

Enterprise Storage Arrays

EVA	StorageWorks Enterprise Virtual Array 8400, 8100, 8000, 6400, 6100, 6000, 5000, 4400, 4100, 4000, 3000, P6500, P6300
MSA	StorageWorks Modular Storage Array 1000, 1500 (NOTE: OpenVMS support for the MSA1500 requires a minimum MSA firmware of Version 7.), MSA2000fc G2, P2000 G3 FC, P2000 G3 FC/iSCSI Combo (FC Connect)
XP 3PAR	StorageWorks XP Storage Array 128/1024, 48/512, P9500, 10000/12000, 20000/24000 7200, 8200, 8400

Adapters and Switches

MDR	StorageWorks Modular Data Router for connecting SCSI and FC tape devices to a FC switch.
NSR	StorageWorks Network Storage Router for connecting SCSI and FC tape devices to a FC switch.
DSGGA-AA/B	8/16-port Fibre Channel switch
DSGGD	16-port 2 GB Fibre Channel switch
B-Series, M-Series, and C-Series Switches	SAN-based FC Switches as supported by HPE StorageWorks

SAN-attached Tape Libraries

EML-E Series Tape Library	Enterprise Storage Library
ESL-E Series Tape Library	Enterprise Storage LibrarySI
ESL9595	Enterprise Storage Library
ESL9322	Enterprise Storage Library
ESL9326	Enterprise Storage Library
ESL9198	Enterprise Storage Library
MSL2024	Business Class Library
MSL4048	Business Class Library
MSL8096	Business Class Library
MSL5000 Series	Modular Storage Library
MSL6000 Series	Modular Storage Library
VLS 6000	Enterprise Virtual Tape Library
VLS9000	Virtual Tape Library
VLS12000	Virtual Tape Library
D2D4106	D2D backup systems
D2D4112	D2D backup systems
D2D4312	D2D backup systems
D2D4324	D2D backup systems

NOTE: OpenVMS supports both SDLT and Ultrium 460/960 tape drives within HPE StorageWorks Tape libraries. For the latest storage hardware device support with OpenVMS Version 8.4-2L1 on Integrity, please refer to this website: <http://www.hp.com/storage/spock>

Abbreviations

APMP	Adaptive Partitioned Multi-Processing
ATA	AT/Attachment
ATAPI	ATA Packet Interface
COM	Component Object Model
DLT	Digital Linear Tape
DSSI	DIGITAL Storage Systems Interconnect
EISA	Extended Industry Standard Architecture
FDDI	Fiber Distributed Data Interface
FSE	Fast Single Ended (SCSI)
FWD	Fast-Wide Differential (SCSI)
GigE	Gigabit Ethernet
IDE	Integrated Device (or Drive) Electronics
IEEE	Institute of Electrical and Electronics Engineers
I80277	Intel® 82077 PC Compatible Floppy Interface
LVD	Low Voltage Differential
MSCP	Mass Storage Control Protocol
NCS	National Character Set
PCI	Peripheral Component Interconnect
QIC	Quarter Inch Cartridge
RAID	Redundant Array of Independent Disks
RMC	Remote Procedure Call
RMS	Record Management Services
SDI	Standard Drive Interface
SMP	Symmetric Multiprocessing
STI	Standard Tape Interface
TFF	Terminal Fallback Facility
TIE	Translated Image Environment
TMSCP	Tape Mass Storage Control Protocol
USB	Universal Serial Bus
VLM	Very Large Memory
XMI	Extended Memory Interconnect

Software Warranty

This software product is provided by VSI with a 90-day conformance warranty in accordance with the VSI warranty terms applicable to the license purchase.

Copyright © 2016 VMS Software, Inc., Bolton Massachusetts, USA

Confidential computer software. Valid license from VSI required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for VSI products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. VSI shall not be liable for technical or editorial errors or omissions contained herein.

Motif is a registered trademark of The Open Group.

Java is a registered trademark of Oracle and/or its affiliates.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.