VSI OpenVMS Version V8.4-2L1 Cover Letter and Release Notes

This document contains release notes provided with the initial release of VSI OpenVMS Integrity Version 8.4-2L1 (August 2016) as well as release notes that were issued with the VSI OpenVMS Integrity Version 8.4-2L1 Update 1 DVD in August 2019.

October 2019

Preface

VSI OpenVMS Version 8.4-2L1 Cover Letter

VMS Software, Incorporated (VSI) is pleased to introduce the OpenVMS V8.4-2L1 operating system for HPE Integrity server platforms, which is contained on the enclosed VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD. This DVD allows you to perform an installation directly to a 16 Gb Fibre Channel device, update the system disk with all the latest VSI V8.4-2L1 ECO patches and boot a new 16 Gb system disk.

The VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD provides the following enhancements that improve the customer experience when installing on new i6 hardware:

1. Updated instructions on modifying the Host Bus Adapters (HBAs) to make 16 Gb Fibre Channel devices visible for booting.
2. Drivers to make 16 Gb Fibre Channel devices visible from the operating system installation media boot menu.
3. The VSI OpenVMS Integrity V8.4-2L1 Update V1.0 ECO kit (VMS842L1I_UPDATE-V0100) in a directory on the DVD that can be installed via option 7 from the installation menu. The ECO kit contains a consolidated roll-up of previously released patch kits for VSI OpenVMS for Integrity Servers V8.4-2L1.

   Please note:
   - If you are installing this VSI OpenVMS Integrity V8.4-2L1 DVD on a system using 16 Gb fibre HBA, you ***must*** install the Update V1.0 ECO kit in order to boot from or use your 16 Gb Fibre Channel devices.
   - VSI strongly recommends that you install the Update V1.0 ECO kit during the V8.4-2L1 upgrade or installation. Many important software issues are corrected in the Update V1.0 ECO kit. The VSI Support Team will not accept problem reports from systems that do not have this kit installed. You may save future downtime by installing the Update V1.0 ECO kit immediately.

Intended Audience

This document is intended for users of VSI OpenVMS Integrity V8.4-2L1. Before beginning an installation or upgrade of VSI OpenVMS Integrity V8.4-2L1, VSI encourages you to review all cover letters and release notes included in the package.

Document Structure

This document contains the following sections:

- *Installation Dependencies and Sequence*: Describes the order of installation, as well as product dependencies related to VSI OpenVMS Integrity V8.4-2L1 Update 1.
- *New Features*: Describes newly added functionality including how to install VSI OpenVMS Integrity V8.4-2L1 directly via a 16 Gb HBA to a Fibre Channel system disk (FC LUN).
- *Release Notes*: Describes software and documentation problems, restrictions, and corrections. Release notes from previous versions of VSI OpenVMS can be found in the *VSI OpenVMS Version 8.4-2 Cover Letter and Release Notes* document.
- *Guide to Media Addendum*: Describes contents of the VSI OpenVMS V8.4-2L1 Update 1 media kit.

Conventions

This manual contains release notes introduced in the current release as well as notes from previous VSI OpenVMS Integrity releases that still apply to the current release. A subheading for each release note indicates either the version of origin (such as V8.4-2L1) or the version when an old note was last updated. For example, a note from Version 8.4-2 that was revised for Version 8.4-2L1 will be labeled with V8.4-2L1.

Notes from previous versions are published when:

- The information in the release note has not been documented in any other VSI OpenVMS document, and the note is still pertinent.
- The release notes may be pertinent in multiple-version OpenVMS Cluster systems.

Installation Dependencies and Sequence

The following notes describe dependencies and recommended installation sequence of several patch kits included on the VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD.

1. **VSI OpenVMS Integrity V8.4-2L1 Update V1.0 ECO kit** (VMS842L1I_UPDATE-V0100): Install this kit first, during the V8.4-2L1 upgrade or installation. Many important software issues are corrected in the Update V1.0 ECO kit.

   Note: The VSI Support Team will not accept problem reports from systems that do not have the Update V1.0 ECO kit installed. You may save future downtime by installing the Update V1.0 ECO kit immediately.

2. **VSI NOTARY V2.0 Patch kit**: This kit is included in the VSI Integrity V8.4-2L1 Update V1.0 ECO kit and will be automatically installed as part of that update. All VSI OpenVMS patch kits now require installation of the VSI NOTARY V2.0 patch kit for their respective version of VSI OpenVMS. This kit ensures correct validation regardless of the manifest version in use.

3. **VSI Enhanced Password Management Software**: If you plan to use the VSI Enhanced Password Management Software for VSI OpenVMS, you must first re-install the VSI NOTARY V2.0 patch kit on top of the VSI OpenVMS Integrity V8.4-2L1 Update V1.0 ECO kit. Once the NOTARY V2.0 has been re-installed, you may install the VSI Enhanced Password Management Software kit. For access to the VSI Enhanced Password Management Software, please contact your support channel.

New Features

1. Installing VSI OpenVMS V8.4-2L1 Directly to a Fibre Channel System Disk

Version 8.4-2L1 Update 1

With the release of the VSI OpenVMS Version 8.4-2L1 Operating Environment Update 1 DVD, you can install the VSI OpenVMS Integrity operating environment directly to a Fibre Channel system disk (FC LUN) via a 16 Gb HBA.

Please refer to the *VSI OpenVMS 16 Gb Fibre Channel HBA Configuration Guide* which is located on the Update 1 DVD in the following directory:

<DVD_DEVICE>:[VMS842L1I_UPDATE.DOCUMENTATION]ENABLING_16GB_FC_HBAS_FOR_BOOT.PDF

Note: The above file specification has a filename that differs from the document's actual title. It is a carryover from a prior SCSI kit and is used for compatibility. Use your favorite browser or PDF viewer to view the file.

To install the VSI OpenVMS V8.4-2L1 operating environment via a 16 Gb HBA, follow these steps:

1. Engage your SAN team to connect the fibre ports from the 16 Gb HBA on the server to the Fibre Channel switches and update switch zoning, if in use.
2. Engage your SAN team to modify the SAN configuration to recognize the new 16 Gb HBA and to enable presentation of the LUNs to the rx2800 i4 or i6 server.
3. Configure your rx2800 i4 or i6 server to boot from your 16 Gb Fibre Channel HBA. Follow the instructions in the section titled *Enabling the 16 Gb HBA for System Booting* on Page 12 in the document *VSI OpenVMS 16 Gb Fibre Channel HBA Configuration Guide*.
4. Boot the V8.4-2L1 Update 1 DVD and install the VSI OpenVMS V8.4-2L1 operating environment to your Fibre Channel LUN.
   Important: Use @SYS$MANAGER:BOOT_OPTIONS.COM to ensure that your boot options are updated to include your new Fibre Channel system disk before moving on to the next step.
5. Follow the instructions in the section titled *Applying the Final HBA Setting* on Page 23 in the *VSI OpenVMS 16 Gb Fibre Channel HBA Configuration Guide*.

2. OpenSSL Update

Version 8.4-2L1

OpenVMS V8.4-2L1 VSI supplements VSI SSL V1.4 with VSI SSL1 V1.0, a new release of OpenSSL for OpenVMS. All OpenVMS components in this release that are dependent on OpenSSL have been modified to make use of the new SSL1 offering.

If you do not require updated SSL support, you need not upgrade to VSI OpenVMS V8.4-2L1. However, if you require support for OpenSSL on any VSI OpenVMS version, VSI recommends that you upgrade to OpenVMS V8.4-2L1.

These SSL-related software components are updated in VSI OpenVMS V8.4-2L1:

- OpenVMS V8.4-2L1 with updates to ENCRYPT, ACME, ACMELDAP
- VSI SSL1 V1.0
- VSI TCP/IP V5.7ECO5F
- VMS Notary
- CSWS (Apache)
- Enterprise Directory (X.500)
- WBEM

VSI's previous version of SSL (SSL V1.4) is based on the OpenSSL.org code base 0.9.8, which is no longer supported by the OpenSSL community. Many commercial applications and operating systems reject communication to OpenSSL 0.9.8 based targets. Deficiencies in the OpenSSL 0.9.8 feature can be addressed by updating to the OpenSSL V1.0.2 code base.

OpenSSL is used by many operating system functions, networking products, OpenVMS layered products, and open source applications. The prevalence of usage makes OpenSSL a default installation option on OpenVMS systems. OpenVMS V8.4-2L1 is a coordinated release of OpenSSL V1.0.2 and all software components that use it. This delivery strategy simplifies release packaging and testing and avoids the possibility of complicated patch dependencies.

Note that VSI SSL V1.4 remains unchanged in this release in order to allow existing customer applications to continue to run. VSI SSL1 V1.0 is designed to co-exist in parallel with VSI SSL V1.4. OpenSSL V1.0.2 is not 100% compatible with V0.9.8, contains new functions and features, and has minor routine interface changes to existing functions. Existing source code may require some minor modifications in order to work with V1.0.2.

VSI OpenVMS V8.4-2L1 is designed to be compatible with, and allow seamless upgrades from, HPE OpenVMS releases, including systems that have had the HPE SSL1 set of patches installed.

NOTE: Customers are encouraged to migrate their existing SSL based applications to use VSI SSL1 V1.0 as soon as practical. VSI will end support for VSI SSL V1.4 in the next release after VSI OpenVMS V8.4-2L1.

3. VSI Secure Web Server V2.4-3 for OpenVMS (based on Apache)

Version 8.4-2L1

VSI is pleased to provide a new VSI-supported version of Secure Web Server (SWS) for OpenVMS based on Apache HTTP Server Version 2.4-12 from the Apache Software Foundation.

SWS V2.4-3 represents a significant update from previous versions, providing many new features and numerous enhancements including reduced memory utilization and more flexible configuration. New loadable modules provide new and enhanced functionality in areas such as session management, request filtering, rate limiting, and proxying. SWS V2.4-3 also provides improved support for the development of custom loadable modules.

SWS V2.4-3 includes Secure Sockets Layer (SSL) MOD_SSL and OpenSSL based on OpenSSL 1.0.2h, thus supporting higher levels of encryption than those provided by previous versions. This helps ensure greater levels of security for clients connecting to your web server on VSI OpenVMS.

Please see http://httpd.apache.org/docs/2.4/new_features_2_4.html for a list of new features, enhancements, and new and changed modules in Apache HTTP Server 2.4. Note that not all new features are provided with Secure Web Server for VSI OpenVMS.

4. VSI VMS Notary V1.2

Version 8.4-2L1

The VMS Notary, part of the OpenVMS operating system, has been updated to use OpenSSL V1.0.2 (SSL1). The VMS Notary allows VSI-signed kits to validate on OpenVMS systems, just as the HPBINARYCHECKER allows HPE-signed kits to validate on OpenVMS.

Release Notes

1. AUTOGEN May Yield Spurious Error Message %SYSTEM-W-NOSUCHDEV

Version 8.4-2L1

As part of the VSI OpenVMS installation and upgrade procedure, an initial boot of a newly created or updated system disk is performed so that AUTOGEN may calculate any necessary changes for system parameters. After AUTOGEN is complete, the system is rebooted using the normal system startup and customer-specific startup procedures.

The following error message may occur during the initial AUTOGEN:

%SYSTEM-W-NOSUCHDEV, no such device available

This error may be safely ignored; there is no detrimental effect on AUTOGEN. The message only appears during the very initial AUTOGEN. Once the system is booted normally the message will not recur.

The error will be corrected in a future release of VSI OpenVMS.

2. Booting VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD From Cell-based HPE Integrity Servers is Unsupported

Version 8.4-2L1

VSI currently does not support booting the VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD from DVD drives on cell-based HPE Integrity Servers such as rx7640 and rx8640, due to a problem with the boot drivers. Please contact support@vmssoftware.com for alternative installation procedures on cell-based systems. This problem will be fixed in a future version.

3. Differences Between VSI OpenVMS V8.4-2L1 and VSI OpenVMS V8.4-2

Version 8.4-2L1

Aside from updated SSL support, VSI OpenVMS Version V8.4-2L1 is identical to VSI OpenVMS Version V8.4-2 with the following patch kits included:

- VMS842I_IMGACT-V0100
- VMS842I_PRCMGT-V0100
- VMS842I_RMS-V0200
- VMS842I_SCSI-V0100
- VMS842I_SYS-V0100
- VMS842I_VMSINSTAL-V0100

There are no other functional differences between these versions of OpenVMS. The patch kits address the following problems:

A. VMS842I_IMGACT-V0100

Abstract: Image activation fails with LOADER-F-NO_SUCH_IMAGE

In certain cases the image activator issues an error message for a file that already exists:

```
%DCL-W-ACTIMAGE, error activating image <image-name>
-CLI-E-IMGNAME, image file <full-file-specification>
-LOADER-F-NO_SUCH_IMAGE, the requested image cannot be located
```

B. VMS842I_PRCMGT-V0100

Abstract: OpenVMS V8.4-2 systems may crash with CWSERR bugcheck

A problem with Special Kernel AST handling within the OpenVMS executive may cause a system crash with a CWSERR bugcheck. Since there is no particular method to determine if a given workload could encounter this issue, VSI recommends that all customers running VSI OpenVMS V8.4-2 systems install this patch kit as a preventative measure.

The bugcheck summary information presented by CLUE CRASH for this problem will have a footprint similar to the following:

```
Bugcheck Type:   CWSERR, Error detected while processing cluster-wide
           service request
Node:                  <nodename>
CPU Type:              <CPU type>
VMS Version:           V8.4-2
Current Process:       <process name>
Current Image:         <image name>
Failing PC:            FFFFFFFF.805792D0 EXE$NAM_TO_PCB_SCHED_C+00670
Failing PS:            00000000.00000200
Module:                PROCESS_MANAGEMENT
Offset:                000BA7D0
```

C. VMS842I_RMS-V0200

Abstract: Fix RMS bugchecks when using RMS Global Buffers

A customer site experienced periodic RMS bugchecks with RMS Global Buffers enabled on RIGHTSLIST.DAT and SYSUAF.DAT. This resulted in deletion of the process that incurred the exception, with the following message:

```
%RMS-F-BUG, fatal RMS condition (FFFFFFC0), process deleted
```

This corresponds to the error "BADGBH, Bad Global Buffer Header found" when the RMS Global Buffer is used for opening a file. After this error occurred, the user could no longer log in and a reboot was required to clear the issue.

This fix addresses a small timing window between instructions if a regular file close (or image rundown) is interrupted by a last chance abort rundown.

Abstract: Remove RMS executive mode alignment faults

A structure used during RMS name processing is built dynamically on the stack. The base structure definition assumed this would always be quadword aligned, however the stack may only be longword aligned.

By enforcing only longword alignment for this structure, the proper instructions are generated to access it without alignment faults, and with no additional instruction overhead. The routines using this structure are accessed repeatedly during RMS Recovery Unit Journal processing. Other RMS operations may also incur these alignment faults depending on your workload.

This patch kit removes these RMS alignment faults, yielding much improved system performance for these operations.

D. VMS842I_SCSI-V0100

Abstract: INVEXCPTN system crash for some SCSI configurations

Some Itanium systems using the LSI53C1030 SCSI tape controller may crash with the following bugcheck:

```
        INVEXCEPTN, Exception while above ASTDEL
```

The I/O devices on the controller affect the exposure risk for this problem.

E. VMS842I_SYS-V0100

Abstract: CPUs are incorrectly distributed among interleaved RADs on i4 BL890c

At boot time, the CPUs on a system are distributed among the RADs (Resource Allocation Domains) for optimal performance. Previously, some CPUs on i4 BL890c servers could be allocated to the wrong interleaved RAD or to no RAD at all, leading to non-optimal performance.

Abstract: SDA CLUE command failure on some Itanium servers

CLUE$SDA may ACCVIO when analyzing a crash dump. The CLUE CONFIG command is most likely to encounter this issue, but other CLUE commands may also fail sporadically. The visible behavior of SDA results in image termination with a message similar to this:

```
    %SYSTEM-F-ACCVIO, access violation, reason mask=04,
                      virtual address=<value>, PC=<value>, PS=<value>
```

If you use CLUE to analyze crash dumps for OpenVMS V8.4-2, install this patch.

F. VMS842I_VMSINSTAL-V0100

Abstract: VMSINSTAL failure on disks with over 1TB of free space

If the system disk free space exceeds 1TB, product installation using the VMSINSTAL mechanism may fail with this message:

```
 %CONWRKSSSL-F-NOSYSSPACE, system disk does not contain enough
     free blocks for installation
```

This is caused by limits of 32-bit arithmetic in DCL. The fix corrects the calculation method, allowing installation to very large disks.

4. Patch Kit Installations May Invalidate Recovery Data for Previously Installed Patch Kits

Version 8.4-2L1

Installing some patch kits (for instance, CSWS, SAMBA, SSL1) will invalidate the saved recovery data for any previously installed patch or patches. (A recovery data set is created when a patch kit is successfully installed with the /SAVE_RECOVERY_DATA qualifier; these data sets are used to uninstall patches when you use the PRODUCT UNDO PATCH command.) Once patch recovery data is deleted, you cannot uninstall any patch that is associated with this data.

Plan your patch kit installations carefully and use system backups liberally in order to avoid a situation where you need to uninstall a patch (or multiple patches). The corresponding recovery data sets may no longer be available.

5. VSI Enterprise Directory V5.8

Version 8.4-2L1

Enterprise Directory V5.8 contains support for Secure Socket Layer (SSL) V1.0.2. Note that Enterprise Directory V5.8 will not work with the SSL 0.9.8 code base. If you need to use SSL 0.9.8, continue to use VSI Enterprise Directory V5.7, which is functionally equivalent to VSI Version 5.8.

6. VSI OpenVMS Installation May Repeat Post-Installation Task Notification

Version 8.4-2L1

Products that have multiple dependencies on other products may display required post-installation tasks more than once during kit installation. This happens because PCSI uses a recursive method to ensure that all dependencies are found, but it does not screen previous dependencies under all circumstances. You can safely ignore the duplicated displays; follow the instructions only once. VSI will address this behavior in a future release.

7. VSI OpenVMS Upgrade Paths

Version 8.4-2L1

VSI supports upgrades to VSI OpenVMS V8.4-2L1 from previous versions of VSI OpenVMS, as well as from HPE OpenVMS v8.4 (with U900, U1000, or U1100 applied), HPE OpenVMS v8.3-1H1 and HPE OpenVMS v8.3.

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

Note: VSI does not support upgrades to VSI V8.4-1H1 or VSI V8.4-2 from systems running HPE OpenVMS v8.4 with HPE SSL1 applied. This is because VSI V8.4-1H1 and VSI V8.4-2 do not provide updated SSL1 support; you would downgrade your SSL functionality. If you run HPE OpenVMS v8.4 and HPE SSL1, upgrade to VSI OpenVMS V8.4-2L1, which provides the updated SSL1 support.

8. VSI TCP/IP V5.7ECO5F

Version 8.4-2L1

The TCPIP57ECO5F kit (VSI-I64VMS-TCPIP-V0507-13ECO5F-1) included with VSI OpenVMS V8.4-2L1 is comprised of a base kit, an ECO kit, and two patch kits. After you install the base TCPIP57ECO5F kit, release notes for the component kits will be located in these locations in SYS$HELP:

Component	**Release Note Location**
TCPIP 5.7	SYS$HELP:TCPIP057.RELEASE_NOTES
TCPIP 5.7 ECO5	SYS$HELP:TCPIP57ECO05.RELEASE_NOTES
TCPIP Telnet Patch	SYS$HELP:TCPIP_TELNET_PAT57ECO05A.RELEASE_NOTES
TCPIP CVE Patch	SYS$HELP:TCPIP_CVE_PAT-V57ECO5.RELEASE_NOTES

A. VSI TCP/IP$CONFIG.COM Support for SSH RSA Host Keys

TCPIP$CONFIG.COM now prompts for the host key type when generating an SSH host key; previously it generated only DSA host keys.
Use of an RSA host key allows connectivity with newer SSH client implementations without requiring reconfiguration of the client to support the older DSA host key types.

Here is an example:

```
        SSH Configuration

        Service is defined in the SYSUAF.
        Service is defined in the TCPIP$SERVICE database.
        Service is not enabled.
        Service is stopped.

             SSH configuration options:

                  1 - Enable service on this node

                  2 - Enable & Start service on this node

                 [E] - Exit SSH configuration

        Enter configuration option: 1
        * Create a new default server host key? [NO]: yes
        * Please enter host key type DSA or RSA [RSA]:
             Creating private RSA key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY
             Creating public RSA key file:
TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY.PUB

        The SSH CLIENT is enabled.

        * Do you want to configure SSH CLIENT [NO]:
```

If an existing key has been in use, SSH clients might refuse connection to the host after you change the key. To correct this, remove the previously used key from the client's list of known keys. Refer to your SSH client documentation for instructions on how to remove keys.

B. VSI TCP/IP NFS Patch Kit

The VSI TCP/IP V5.7 product includes the NFS kit VSI-I64VMS-TCPIP_NFS_PAT-V0507-ECO5C-4, which is an optional kit that can be selected during the VSI TCP/IP kit installation. This patch kit resolves a problem seen when the /ADF option is used to mount an NFS file system residing on some non-OpenVMS file servers. In this situation, file attributes are not properly written when copying files to the NFS file system. Here is an example of the incorrect behavior:

```
TBD_$ tcpip MOUNT DNFS100: /adf /HOST="10.5.117.2" /PATH="/usr/nfs-test" /system
TBD_$ backup /log test.txt dnfs100:[NFS-TEST]test.txt
```

```
%BACKUP-S-CREATED, created DNFS100:[NFS-TEST]TEST.TXT;3
%BACKUP-W-WRITEERR, error writing DNFS100:[NFS-TEST]TEST.TXT;2
-SYSTEM-W-FCPWRITERR, file processor write error
%BACKUP-E-WRITEATTR, error writing attributes for DNFS100:[NFS-TEST]TEST.TXT;2
-SYSTEM-W-FCPWRITERR, file processor write error
%BACKUP-S-CREATED, created DNFS100:[NFS-TEST]TEST.TXT;2
%BACKUP-W-WRITEERR, error writing DNFS100:[NFS-TEST]TEST.TXT;1
-SYSTEM-W-FCPWRITERR, file processor write error
%BACKUP-E-WRITEATTR, error writing attributes for DNFS100:[NFS-TEST]TEST.TXT;1
-SYSTEM-W-FCPWRITERR, file processor write error
%BACKUP-S-CREATED, created DNFS100:[NFS-TEST]TEST.TXT;1
```

C. VSI TCP/IP SSH Patch Kit Addresses Multiple Problems

The VSI TCP/IP V5.7 product includes the SSH patch kit VSI-I64VMS-TCPIP_SSH_PAT-V0507-ECO5D-4 which is an optional kit that can be selected during the VSI TCP/IP kit installation. The patch kit addresses the following problems:

1. When authenticating an LDAP user account using RedHat/Fedora Directory Server, the server may send password expiration warning in the Bind Response using Netscape controls. But for SSH sessions, the respective warning message doesn't get displayed in OpenVMS at login time.
2. Installing the ACMELOGIN images (included in LOGINPLUS kit) is a pre-requisite for LDAP authentication. However, with ACMELOGIN installed, the SET PASSWORD command will not work in SSH sessions, even though it works fine in other terminals like Telnet, DECnet, etc. This restriction is documented in the VSI TCP/IP 5.7 ECO5 release notes, as well as the ACME LDAP Installation Guide.

   To overcome this limitation, define the following logical before starting SSH server:

   ```
   $ DEFINE  /SYSTEM  TCPIP$SSH_SERVER_USE_LOGINOUT  1
   ```

   This prompts SSH server to use [SYSEXE]LOGINOUT.EXE image for authentication (as is done in Telnet and DECnet terminals). Now the "SET PASSWORD" command will work fine in SSH sessions.

   Please note that enabling this feature has following side effects:

   a) The LOGINOUT component will display a default Welcome message if SYS$WELCOME logical is not defined. This is the behavior in Telnet, DECnet, etc. since they use LOGINOUT. On the other hand, SSH server will not display any Welcome message if SYS$WELCOME logical is not defined. Enabling TCPIP$SSH_SERVER_USE_LOGINOUT will cause SSH server to behave like Telnet - i.e. display a default Welcome message when SYS$WELCOME is undefined.

b) By default, the Audit server logs the LOGIN event for DCL process in SSH session as "Detached process login". But if TCPIP$SSH_SERVER_USE_LOGINOUT is enabled, the respective event will be "Local interactive login".

c) In the case of LDAP users, the ACME server will perform user-authentication twice if TCPIP$SSH_SERVER_USE_LOGINOUT is enabled - the first one initiated by SSH server, and the second one by LOGINOUT image. Hence the timestamp "Last interactive login" displayed at start of interactive session will be almost same as the current time. This is because the timestamp is updated twice in quick succession by the ACME server.

d) The logical TCPIP$SSH_SERVER_USE_LOGINOUT doesn't take effect in the following scenarios:
- SSH sessions using remote command mode
- SFTP/SCP sessions
- SSH logins using public-key or host-based authentication
- OpenVMS users with secondary password

e) While displaying the Welcome message, width of the terminal may be limited to 80 characters, if LOGINOUT is enabled.

3. For an LDAP user, if the password has already expired, then the SSH authentication simply fails without any indication of password expiry.

   Note:The primary reason for this issue is a bug in the ACME LDAP agent. Hence this issue is not exclusive to SSH; it occurs even in Telnet, DECnet, as well as the system console prompt. VMS Security Engineering will release a patch for ACME LDAP agent to address this issue (Elevation: QXCM1001425603 / 4754317355). However, to prevent the problem in SSH sessions, a few related changes are required in the SSH server as well. Hence for SSH users, both ACME LDAP agent patch as well as the SSH server patch (V5.7-ECO5D) must be installed in the system.

4. SSH connections from a client which mandates support for the diffie-hellman-group14-sha1 key exchange method fail.

9. VSI WBEMCIM

Version 8.4-2L1

VSI WBEM Services V3.0 is required for compatibility with the VSI SSL1 product. VSI SSL1 updates OpenVMS SSL to the OpenSSL V1.0.2h version.

VSI WBEM Services V3.0 will install on any VSI OpenVMS system with VSI SSL1 installed.

10. VSI WBEM Providers

Version 8.4-2L1

VSI WBEM Providers V2.2-5c is required for compatibility with the VSI SSL1 product. VSI SSL1 updates OpenVMS SSL to the OpenSSL V1.0.2h version.

VSI WBEM Providers V2.2-5c will install on any VSI OpenVMS system with VSI SSL1 installed.

Guide to Media Addendum

The VSI OpenVMS Integrity V8.4-2L1 media kit contains the following items:

Media	Part Number
VSI OpenVMS Integrity Version 8.4-2L1 Update 1 Operating Environment DVD	ME-VIBHU1-001
VSI OpenVMS Documentation CD	ME-VIADOC-01A
VSI OpenVMS Version 8.4-2 Layered Products DVD	ME-VIBHAC-002
VSI TCP/IP for OpenVMS Version 10.6 DVD	ME-MVITCP-02A
Documentation	**Part Number**
VSI OpenVMS Version 8.4-2L1 Cover Letter and Release Notes (this document)	DO-VIBHAD-003
VSI OpenVMS Version 8.4-2 Cover Letter and Release Notes	DO-VIBHAC-001
VSI OpenVMS Version 8.4-2 Installation and Upgrade Manual	DO-VIBHAB-002
VSI OpenVMS Documentation CD Cover Letter and Guide to Media	DO-DVIACL-01A
End User License Agreement (EULA)	DO-VIEULA-001
VSI OpenVMS Version 8.4-2 Guide to Media	DO-VIBHAC-003
VSI TCP/IP for OpenVMS Version 10.6 Cover Letter	DO-DVTCLR-01A
VSI OpenVMS 16 Gb Fibre Channel HBA Configuration Guide	DO-DVICNG-01A
Important Information When Migrating from HPE OpenVMS to VSI OpenVMS	DO-DUPCVR-01B

VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD Contents

Contents of the DVD include the following:

- VSI OpenVMS Integrity V8.4-2L1 operating environment, including layered products
- VSI OpenVMS Integrity V8.4-2L1 Update V1.0 ECO kit (VMS842L1I_UPDATE-V0100). Review the ECO kit's release notes *VMS842L1I_UPDATE-V0100.RELEASE_NOTES* for a kit description, installation requirements, and complete list of patches included in the kit.
- Drivers to make 16 Gb Fibre Channel devices visible from the operating system installation media boot menu.
- VSI OpenVMS V8.4-2L1 documentation, including these items:
  - *VSI OpenVMS Integrity V8.4-2L1 Update 1 DVD Cover Letter and Release Notes.*
  - *VSI OpenVMS 16 Gb Fibre Channel HBA Configuration Guide*
  - All original VSI OpenVMS Integrity V8.4-2L1 documentation, as well as an updated *VSI OpenVMS Integrity V8.4-2L1 Software Product Description*.

Table 1 lists product names, version numbers, and directories found on the VSI OpenVMS Version 8.4-2L1 Update 1 Operating Environment DVD. Before you perform an installation or upgrade with the VSI OpenVMS V8.4-2L1 Update 1 DVD, please review the following documents.

- *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*

Table 1 Products on VSI OpenVMS Integrity Version 8.4-2L1 Update 1 Operating Environment DVD

VSI Product Name	Version	Directory
VSI Another Neat Tool (ANT)	1.7-1B	[KITS.ANT_KIT]
VSI Availability Manager	3.2	[KITS.AVAILMAN_KIT]
VSI Availability Manager Base	3.2	[KITS.AVAIL_MAN_BASE_KIT]
VSI AXIS2	1.1-1	[KITS.AXIS2_KIT]
VSI CDSA	2.4-322A	[KITS.CDSA]
VSI Common Internet File System (CIFS)	1.2-ECO1A	[KITS.CIFS_KIT]
VSI DECnet Phase IV	8.4-2L1	[KITS.DECNET_PHASE_IV_I640842L1_KIT]
VSI DECnet Plus, including FTAM, VT, OSAK	8.4C	[KITS.DECNET_PLUS]
VSI DECprint Supervisor (DCPS)	2.8	[KITS.DCPS_KIT]
VSI DECwindows Motif	1.7E	[KITS.DWMOTIF]
VSI DECwindows Motif Support	1.7E	[KITS.DWMOTIF_SUPPORT_I640842L1_KIT]
VSI Distributed Computing Environment (DCE RT)	3.2A	[KITS.DCE_KIT]
VSI Enterprise Directory	5.8	[KITS.ENTERPRISE_DIR_KIT]
VSI HPBINARYCHECKER	1.2	[KITS.HPBINARYCHECKER]
VSI I18N	8.4-2L1	[KITS.I18N_KIT]
VSI Kerberos	3.2-260	[KITS.KERBEROS]
VSI Perl	5.20-2A	[KITS.PERL_KIT]
VSI Secure Sockets Layer 1 (SSL1)	1.0	[KITS.SSL1]
VSI Secure Sockets Layer (SSL)	1.4-503	[KITS.SSL]
VSI Secure Web Server (CSWS)	2.4-3	[KITS.CSWS_KIT]
VSI Secure Web Server CSWS_JAVA	7.0-29B	[KITS.CSWS_JAVA_KIT]
VSI Secure Web Server CSWS_PHP	5.2-17A	[KITS.CSWS_PHP_KIT]
VSI TCP/IP	5.7-13ECO05F	[KITS.TCPIP]
VSI TDC_RT	2.3-1120	[KITS.TDC_RT]
VSI UDDI	1.0-B	[KITS.UDDI_KIT]
VSI OpenVMS Version 8.4-2L1 Update 1 ECO	1.0	[KITS.VMS842L1I_UPDATE_KIT]
VSI WBEM/CIM	3.0-C160513	[KITS.WBEMCIM]
VSI WBEM Providers	2.2-5c	[KITS.WBEMPROVIDERS]
VSI WSIT	3.4-1-1	[KITS.WSIT_KIT]
VSI XML_JAVA	4.0-1	[KITS.XML_JAVA]
XML C for VSI OpenVMS[1]	3.0-1-1	[KITS.XML_CXX_KIT]

[1] While the kit name displays as XML_C, the kit contains XML_C++.

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.