VMS Software

VSI TCP/IP Services for OpenVMS V6.0-25 Release Notes

Software Version: VSI TCP/IP Services for OpenVMS Alpha V6.0-25
VSI TCP/IP Services for OpenVMS Integrity V6.0-25
VSI TCP/IP Services for OpenVMS x86-64 V6.0-25

VMS Software, Inc. (VSI)
Boston, Massachusetts, USA

VSI TCP/IP Services for OpenVMS V6.0-25 Release Notes

Legal Notice

Table of Contents

Preface

1. Intended Audience

This document is intended for all users of VSI OpenVMS Alpha, VSI OpenVMS Integrity, and VSI OpenVMS x86-64.

2. Prerequisites

VSI TCP/IP Services for OpenVMS Alpha V6.0-25 can be installed on an Alpha system running VSI OpenVMS V8.4-2L1 or VSI OpenVMS V8.4-2L2.

VSI TCP/IP Services for OpenVMS Integrity V6.0-25 can be installed on an Integrity system running VSI OpenVMS V8.4-2L1 or VSI OpenVMS V8.4-2L3.

VSI TCP/IP Services for OpenVMS x86-64 V6.0-25 can be installed on an x86-64 system running VSI OpenVMS V9.2-1 or higher. If you are using VSI OpenVMS V9.2-1, VSI recommends that you upgrade to the latest version.

VSI SSL3 V3.0-7 or later must be installed on the system on which you are planning to install VSI TCP/IP Services for OpenVMS V6.0-25.

Release Notes

VMS Software, Inc. (VSI) is pleased to introduce VSI TCP/IP Services for OpenVMS Alpha V6.0-25, VSI TCP/IP Services for OpenVMS Integrity V6.0-25, and VSI TCP/IP Services for OpenVMS x86-64 V6.0-25.

These products (referred to as VSI TCP/IP Services V6.0 later on in this document) are the VSI implementation of the TCP/IP networking protocol suite and internet services for OpenVMS Alpha, OpenVMS Integrity, and OpenVMS x86-64 systems respectively. VSI TCP/IP Services V6.0 provides a comprehensive suite of functions and applications that support industry-standard protocols for heterogeneous network communications and resource sharing.

This document provides a general overview of VSI TCP/IP Services V6.0 and lists the updated features and known issues.

If you encounter any issues with VSI TCP/IP Services V6.0, please report them to VSI support.

For detailed information on running the TCPIP$CONFIG configuration procedure, refer to the *VSI TCP/IP Services for OpenVMS Installation and Configuration* [https://docs.vmssoftware.com/vsi-tcpip-services-for-openvms-installation-and-configuration/] manual.

1. Available Services

The following services are available in VSI TCP/IP Services V6.0:

- BIND [1]
- DHCP Client
- FTP
- FTPS
- Finger
- FailSafe IP
- IMAP (not yet available on x86-64, applies to IA64 and Alpha, only)
- LBROKER
- LPR/LPD
- NFS
- NTP4
- POP

[1] VSI TCP/IP Services V6.0 uses the BIND 9.11.37 Server. Managing the BIND TCP/IP service is documented in the *VSI TCP/IP Services for OpenVMS Management* [https://docs.vmssoftware.com/vsi-tcpip-services-for-openvms-6-management/] manual.

- Remote (R) Commands
- SMTP
- SNMP
- Socket API
- TELNET (except Kerberos authentication)
- XDM

Note

VSI TCP/IP Services V6.0 kit *does not* include an SSH component. However, if you need to use SSH in your environment, VSI recommends that you use the latest available version of VSI OpenSSH.

2. Known Issues And Limitations

This section lists the known issues and limitations in VSI TCP/IP Services V6.0.

2.1. VSI FTP Service Might Not Connect Correctly In Virtual Environments With NAT Enabled

If the FTP service does *not* work after it has been started, switch to passive mode with the following command:

```
FTP> SET PASSIVE ON
Passive is ON
```

In passive mode, the FTP client always initiates a data connection. This is useful in virtual machine environments when there is network address translation (NAT) in your network.

To run this command automatically when you invoke FTP, put it into SYS$LOGIN:FTPINIT.INI. For the full description of the SET PASSIVE command, refer to the *VSI TCP/IP Services for OpenVMS User's Guide* [https://vmssoftware.com/docs/VSI_TCPIP_SERVICES_UG.pdf].

2.2. Running DHCP Client And failSAFE IP Are Not Compatible on the Same NIC

You cannot run the DHCP and the failSAFE IP client on the same NIC on VSI TCP/IP Services V6.0. If a customer is running the DHCP client on a NIC, then failSAFE IP should not be configured on this NIC, because since the address assignment is controlled by DHCP, there is always the possibility that the address could change. If a customer needs to run the DHCP client and provide a failover mechanism, they should configure the NIC in a LAN failover set.

2.3. NTPDATE No Longer Supported

NTPDATE is no longer supported and will be removed from an upcoming release of VSI TCP/IP Services V6.0. To perform the equivalent of NTPDATE, run `NTPD` making use of the `-q` and `"-G"` options.

```
$ ntpd :== $tcpip$ntp
$ ntpd "-G" -q
ntp.exe[538969120]: ntpd 4.2.8p15@1.3728 Fri Sep 22 07:00:58 UTC 2020 (2): Starting
ntp.exe[538969120]: Command line: tbd$dka200:[sys0.syscommon.][sysexe]tcpip$ntp.exe -
G -q -4
ntp.exe[538969120]: ----------------------------------------------------
ntp.exe[538969120]: ntp-4 is maintained by Network Time Foundation,
ntp.exe[538969120]: Inc. (NTF), a non-profit 501(c)(3) public-benefit
ntp.exe[538969120]: corporation.  Support and training for ntp-4 are
ntp.exe[538969120]: available at https://www.nwtime.org/support
ntp.exe[538969120]: ----------------------------------------------------
ntp.exe[538969120]: proto: precision = 1000.000 usec (-10)
ntp.exe[538969120]: proto: fuzz beneath 0.710 usec
ntp.exe[538969120]: basedate set to 2022-05-21
ntp.exe[538969120]: gps base set to 2022-05-22 (week 2211)
ntp.exe[538969120]: Listen and drop on 0 v4wildcard 0.0.0.0:123
ntp.exe[538969120]: Listen normally on 1 LO0 127.0.0.1:123
ntp.exe[538969120]: Listen normally on 2 WE0 10.10.116.182:123
ntp.exe[538969120]: Listening on routing socket on fd #4 for interface updates
ntp.exe[538969120]: ntpd: time set -50.590756 s
ntpd: time set -50.590756s
$
```

2.4. TCPIP$BIND_CONF.TEMPLATE_FORWARD Requires Adjustment in Environments Not Supporting DNSSEC

The following lines in the TCPIP$BIND_CONF.TEMPLATE_FORWARD template file set up the forwarders' addresses and the DNSSEC validation:

```
//Specifies the IP addresses to be used for forwarding.
//The default is the empty list (no forwarding).
forwarders {
    8.8.8.8;
    8.8.4.4;
};

dnssec-validation auto; //Enable DNSSEC validation.
                        //Note dnssec-enable also needs to be set to
                        //yes to be effective. The default is yes.
```

However, if forwarders are changed to DNS servers that do not support DNSSEC or have it disabled, DNS lookup replies will be discarded when the DNSSEC validation fails.

To avoid this, comment out the following line:

```
dnssec-validation auto
```

2.5. NFS Client Issues

2.5.1. File Attribute Issues in Stress Testing

Occasionally, the attributes of a file just written from a client under stress testing are briefly inconsistent with the server's copy, despite having been properly stored on the server.

2.5.2. SS$_BADIRECTORY Error When Deleting a File

The error SS$_BADIRECTORY is occasionally returned when deleting a file.

2.5.3. Recommending an Extended Timeout Value

The default timeout value of 1 second is problematic. It is recommended that a larger timeout value is used (5 seconds), and a future release will increase the default value.

2.5.4. Stale File Reports in OPCOM with NFS Delete Requests

A stale file is occasionally reported by OPCOM, usually with an NFS client delete request. This problem is usually caused by the client performing the GET ATTRIBUTES operation after the deletion.

2.5.5. QIO Operations May Fail With Timeout Error

The QIO operations on the NFS client may fail with an unexpected TIMEOUT error when the operations on the server side take longer than expected.

One of such situations may occur when VSI OpenVMS is running on a guest virtual machine, and the NFS client sends server requests too frequently. The solution in this case would be to increase the timeout interval to a larger value, around 5 seconds.

The error may also occur when a large file is created on the server side via a CREATE operation that specifies the file size, and the target disk has the **High-Water Marking** feature enabled. To remedy this, there are two options:

- If the security of the disk data is *not* critical, the **High-Water Marking** feature can be disabled.
- If the security of the disk data *is* critical, the **Erase on Delete** feature should be used instead of **High-Water Marking**.

3. Resolved Issues

This section describes the issues that were fixed for this release. For information about the issues that were fixed in previous releases, refer to *VSI TCP/IP Services for OpenVMS V6.0-24 Release Notes* [https://docs.vmssoftware.com/vsi-tcpip-services-for-openvms-6024-release-notes/].

3.1. AF_UNIX BSD44 Sockets Support

The TCPIP socket library contains latent support for AF_UNIX socket types. Previously, this support was limited to non-BSD44 sockets and did not function properly. This issue has been fixed, and now BSD44 sockets are supported. To enable these sockets, you must define the TCPIP $AF_UNIX_MIN_PORT and TCPIP$AF_UNIX_MAX_PORT logical names to establish a port range to be used for this socket type.

3.2. Thread Structure Corruption in NFS Server No Longer Crashes the System

Previously, a problem with the thread management component of the NFS server resulted in corruption of the thread data structure which led to an unexpected page fault while in kernel mode. This problem has been addressed in this release.

4. Upgrading from TCPI/IP Services V5.7

Before upgrading from TCP/IP Services V5.7 to V6.0, you should make several adjustments to your V5.7 configuration using TCPIP$CONFIG:

1. If you are currently using the DHCP server, disable it. This facility is not yet implemented in VSI TCP/IP Services V6.0.

2. If you are currently using the DHCP client, disable it. The DHCP client implementation in VSI TCP/IP Services V6.0 differs from that in V5.7. If you plan to enable the DHCP client after upgrading to V6.0, it will utilize the new configuration logic found in TCPIP$CONFIG.

3. If you are currently using the SSH client, disable it. The SSH client is now part of the VSI OpenSSH product, and is not included in VSI TCP/IP Services V6.0.

4. If you are currently using the SSH server, disable it. The SSH server is now part of the VSI OpenSSH product, and is not included in VSI TCP/IP Services V6.0.

If you had been using the SSH server, you may notice a disabled service definition for SSH in your configuration. If you do not intend to upgrade to the VSI OpenSSH product, you can remove it. Otherwise, consult the release notes for VSI OpenSSH for details on the migration feature included in the product's installation procedure.

Appendix A. Security Enhancements for VSI TCP/IP Services V6.0 FTPS

FTPS (FTP over SSL) allows for an encrypted data connection when using FTP. FTPS is run by using either **FTP /SSL** or **COPY /FTP /SSL** commands.

A.1. Changes in Connection Behavior

With TCP/IP Services V5.7 and prior versions, if you use FTPS and the FTP server is not set up to run SSL by not having the proper certificate, the following messages will be displayed, and the connection will continue in plain text:

```
TCPIP$_FTP_SSLERR, SSL not enabled on server
TCPIP$_FTP_SSLERR, Session will continue in plain text
```

See the following example:

```
$ ftp /ssl node1
220 node1.example.com FTP Server (Version 5.7) Ready.
Connected to node1.
500 AUTH command unsuccessful.
TCPIP$_FTP_SSLERR, SSL not enabled on server
TCPIP$_FTP_SSLERR, Session will continue in plain text
Name (node1:username):

$ copy /ftp /ssl /log node2"username password"::file.txt *.*
TCPIP$_FTP_SSLERR, SSL not enabled on server
TCPIP$_FTP_SSLERR, Session will continue in plain text

%TCPIP-S-FTP_COPIED, NODE2.EXAMPLE.COM"username
password"::file.txt copied to DISK:[USERNAME]FILE.TXT;7
(968408 bytes)
```

With VSI TCP/IP Services V6.0, if you use FTPS and the FTP server is not set up to run SSL, the connection will be terminated. See the following examples:

```
$ ftp /ssl node1
220 node1.example.com FTP Server (Version 5.7) Ready.
Connected to node1.
500 AUTH command unsuccessful.
%TCPIP-E-SSLERR, SSL not enabled on server

$ copy /ftp /ssl /log node2"username password"::file.txt *.*
%TCPIP-E-SSLERR, SSL not enabled on server
```

You must either connect to an SSL-enabled FTP server or reissue the command without the `/SSL` qualifier.

A.2. Changes in Certificate Verification

VSI TCP/IP Services V5.7 and prior versions only check for certificate integrity but do not perform the full server certificate verification. Blindly using a self-signed certificate is not a secure practice.

In the following example, VSI TCP/IP Services V5.7 allows the connection to the FTP server without notifying about the self-signed certificate used by the server.

```
$ ftp /ssl node3
220 node3.example.com FTP Server (Version 5.7) Ready.
Connected to node3.
234 AUTH command successful.
200 PBSZ command successful.
200 PROT command successful.
Name (node3:username):

$ copy /ftp /ssl /log node3"username password"::file.txt *.*
%TCPIP-S-FTP_COPIED, node3"username password"::FILE.TXT;18 copied
to DISK$WORK:[USERNAME]FILE.TXT;19 (1476 bytes)
```

VSI TCP/IP Services V6.0 includes a check for a self-signed or expired server certificate and outputs the appropriate message if such certificates are encountered. You can use a self-signed certificate if you trust the certificate and accept to use it.

The following example shows the connection to the FTP server with a self-signed certificate using VSI TCP/IP Services V6.0:

```
$ ftp /ssl node4
220 node4.example.com FTP Server (Version 6.0) Ready.
Connected to node4.
234 AUTH command successful.
200 PBSZ command successful.
200 PROT command successful.

%TCPIP-F-SSLERR, self signed certificate

       Country: US
         State: MA
      Locality: Boston
  Organization: Certificate Company
          Name: company.com
        E-Mail: first.last@company.com
    Valid from: 30-Apr-2021 22:57
       Expires: 30-Apr-2022 22:57

If you trust the certificate, re-issue the command with the /TRUST
 qualifier.

$ copy /ftp /ssl node3"username password"::file.txt *.*
%TCPIP-F-SSLERR, self signed certificate

       Country: US
         State: MA
      Locality: Boston
  Organization: Certificate Company
          Name: company.com
        E-Mail: first.last@company.com
```

```
    Valid from: 30-Apr-2021 22:57
       Expires: 30-Apr-2022 22:57

If you trust the certificate, re-issue the command with the /TRUST
 qualifier.
```

Add the **/TRUST** qualifier to the command to proceed with the FTPS connection as in the following example:

```
$ ftp /ssl /trust node4
220 node4.example.com FTP Server (Version 6.0) Ready.
Connected to node4.
234 AUTH command successful.
200 PBSZ command successful.
200 PROT command successful.
%TCPIP-I-SSLERR, self signed certificate
%TCPIP-I-SSLERR, TRUST specified; FTP/SSL continuing...
Name (node4:username):

$ copy /ftp /ssl /log /trust node4"username password"::file.txt *.*
%TCPIP-I-SSLERR, self signed certificate
%TCPIP-I-SSLERR, TRUST specified; FTP/SSL continuing...

%TCPIP-S-FTP_COPIED, node4"username password"::FILE.TXT;18 copied to
 DISK:FILE.TXT;22 (1476 bytes)
```