VMS Software

VSI TCP/IP Services Version X6.0 Release Notes

Document Number: DO-TCPRNT-01A

Publication Date: July 2023

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

VSI TCP/IP Services Version X6.0 Release Notes

VMS Software

Copyright © 2023 VMS Software, Inc. (VSI), Boston, Massachusetts, USA

Legal Notice

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.

HPE, HPE Integrity, HPE Alpha, and HPE Proliant are trademarks or registered trademarks of Hewlett Packard Enterprise.

Intel, Itanium and IA-64 are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group.

Preface

1. Intended Audience

This document is intended for all users of VSI OpenVMS Alpha and VSI OpenVMS Integrity.

2. Prerequisites

VSI TCP/IP Services for OpenVMS Alpha Version X6.0-22A can be installed on an Alpha system running VSI OpenVMS 8.4-2L1 or VSI OpenVMS 8.4-2L2.

VSI TCP/IP Services for OpenVMS Integrity Version X6.0-22A can be installed on an Integrity system running VSI OpenVMS 8.4-2L1 or VSI OpenVMS 8.4-2L3.

VSI SSL3 V3.0-7 or later must be installed on the system on which you are planning to install VSI TCP/IP Services Version X6.0-22A.

Release Notes

VMS Software, Inc. (VSI) is pleased to introduce VSI TCP/IP Services for OpenVMS Alpha Version X6.0-22A and VSI TCP/IP Services for OpenVMS Integrity Version X6.0-22A.

These products (referred to as VSI TCP/IP Services X6.0 later on in this document) is the VSI implementation of the TCP/IP networking protocol suite and internet services for OpenVMS Alpha systems and OpenVMS Integrity systems respectively. VSI TCP/IP Services X6.0 provides a comprehensive suite of functions and applications that support industry-standard protocols for heterogeneous network communications and resource sharing.

This document provides the general overview of VSI TCP/IP Services X6.0, as well as lists the updated features and known issues.

1. OpenSSH Is Not Included in VSI TCP/IP Services

VSI TCP/IP Services X6.0 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. Starting VSI TCP/IP Services

Before starting VSI TCP/IP Services, you must run the TCPIP$CONFIG configuration procedure. To start TCPIP$CONFIG, enter the following command:

```
$ @SYS$MANAGER:TCPIP$CONFIG.COM
```

Then, to start the network stack, enter the following command:

```
$ @SYS$STARTUP:TCPIP$STARTUP.COM
```

For detailed information on running the TCPIP$CONFIG configuration procedure, refer to the *VSI TCP/IP Services for OpenVMS Installation and Configuration* manual.

For a configuration example for FTP and TELNET, refer to the *VSI OpenVMS x86-64 V9.2-1 Installation Guide*.

Note

If FTP 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*.

---

3. Available Services

The following services are available in VSI TCP/IP Services X6.0:

- BIND
- DHCP Client
- FTP
- FTPS
- Finger
- FailSafe IP
- IMAP
- LBROKER
- LPR/LPD
- NFS
- NTP4
- POP
- Remote (R) Commands
- SMTP
- SNMP
- Socket API
- TELNET (except Kerberos authentication)
- XDM

If you encounter any issues with VSI TCP/IP Services X6.0, please report them to VSI support.

With VSI TCP/IP Services X6.0, VSI introduces security enhancements for FTPS (FTP over SSL). For details, refer to Section 5.

Before starting VSI TCP/IP Services, you must run the TCPIP$CONFIG configuration procedure. To start TCPIP$CONFIG, enter the following command:

```
$ @SYS$MANAGER:TCPIP$CONFIG.COM
```

To start the network stack after configuring it, enter the following command:

```
$ @SYS$STARTUP:TCPIP$STARTUP.COM
```

For detailed information on running the TCPIP$CONFIG configuration procedure, refer to the *VSI TCP/IP Services for OpenVMS Installation and Configuration* manual.

For a configuration example for FTP and TELNET, refer to the *VSI OpenVMS x86-64 V9.2-1 Installation Guide*.

Note

If FTP 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*.

4. TCP/IP Services Uses BIND 9.11.37 Server

The current version of VSI TCP/IP Services for OpenVMS uses the BIND 9.11.37 Server.

Using Bind 9.11.37 is documented in the *VSI TCP/IP Services for OpenVMS Management* manual. VSI also recommends that users refer to the *Internet Systems Consortium (ISC) website* for the latest updates to Bind 9 configurations and resources.

5. Security Enhancements for VSI TCP/IP Services X6.0 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.

5.1. 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.domain.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.DOMAIN.COM"username
password"::file.txt copied to DISK:[USERNAME]FILE.TXT;7
(968408 bytes)
```

With VSI TCP/IP Services X6.0, 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.domain.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.

5.2. 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.domain.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 X6.0 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 X6.0:

```
$ ftp /ssl node4
220 node4.domain.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.domain.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)
```

6. Known Issues

This section lists the known issues in VSI TCP/IP Services for OpenVMS X6.0.

6.1. 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 for OpenVMS X6.0. If a customer is running the DHCP client on a NIC, then failSAFE IP should not

be configured on this NIC. Since the assigned address is actually controlled by DHCP, VSI TCP/IP Services for OpenVMS should *not* reassign this address. If a customer needs to run the DHCP client and provide a failover mechanism, they should configure the NIC in a lan failover set.

6.2. NTPDATE No Longer Supported

NTPDATE is no longer supported and will be removed from an upcoming release of VSI TCP/IP Services. 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
$
```

6.3. 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, please comment out the line of `dnssec-validation auto`.

6.4. TCPIP MOUNT /SHARE Command Causes a System Hang

When using the TCP/IP 6.0-19D NFS client, entering the command `TCPIP MOUNT /SHARE` will cause the system to hang.

Until this issue is resolved, VSI recommends restricting the access to the NFS mount commands to privileged users only. This can be done by setting the permissions on the SYS$SHARE:TCPIP$DNFS_MOUNT_SHR.EXE file as follows:

```
SET SECURITY/PROTECTION=WORLD SYS$SHARE:TCPIP$DNFS_MOUNT_SHR.EXE
```

6.5. Data Needed for SHOW NETWORK to Report Network Status Is Not Available When Using DHCP Client

When using DHCP client to configure interface(s), the information needed for the command `SHOW NETWORK` to report the TCP/IP network status is not initialized. In this scenario, `SHOW NETWORK` will display the following:

```
$ show network

Product:  TCP/IP    Node:  <TCP/IP host/node name not yet available>
 Address(es):  0.0.0.0
```

If necessary, the missing information may be obtained with one or more options of the `TCPIP SHOW` command.