

VSI TCP/IP Services for OpenVMS V6.0-24 Release Notes

Document Number: DO-TCPRNT-01A

Publication Date: May 2024

Software Version: VSI TCP/IP Services for OpenVMS Alpha V6.0-24
VSI TCP/IP Services for OpenVMS Integrity V6.0-24
VSI TCP/IP Services for OpenVMS x86-64 V6.0-24

VSI TCP/IP Services for OpenVMS V6.0-24 Release Notes



VMS Software

Copyright © 2024 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	v
1. Intended Audience	v
2. Prerequisites	v
Release Notes	1
1. Available Services	1
2. Known Issues And Limitations	2
2.1. VSI FTP Service Might Not Connect Correctly In Virtual Environments With NAT Enabled	2
2.2. Running DHCP Client And failSAFE IP Are Not Compatible on the Same NIC	2
2.3. NTPDATE No Longer Supported	2
2.4. TCPIP\$BIND_CONF.TEMPLATE_FORWARD Requires Adjustment in Environments Not Supporting DNSsec	3
2.5. File Attribute Issues in Stress Testing	3
2.6. SS\$_BADIRECTORY Error when Deleting a File	3
2.7. Recommending an Extended Timeout Value	3
2.8. Stale File Reports in OPCOM with NFS Delete Requests	4
2.9. NFS Server WRITE Error and Occasional Client Request Issue	4
2.10. QIO Operations May Fail With Timeout Error	4
3. Resolved Issues	4
3.1. TCPIP\$CONFIG Fails In Extended Parse Mode	4
3.2. DNFS Client Handling of Servers That Do Not Support READDIRPLUS	4
3.3. DNFS Client Handling of Return Codes From Certain Functions	5
3.4. DNFS Client Fails to Serialize Access to State Data	5
3.5. DNFS Client Handling of Long File Handles	5
3.6. DNFS Client Handling of Odd-Sized File Handles	5
3.7. DNFS Client Handling Failed Memory Allocations	5
4. Upgrading from TCPI/IP Services V5.7	5
Appendix A. Security Enhancements for VSI TCP/IP Services V6.0 FTPS	7
A.1. Changes in Connection Behavior	7
A.2. Changes in Certificate Verification	7

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 V6.0-24 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 V6.0-24 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 V6.0-24 can be installed on an x86 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 V6.0-24.

Release Notes

VMS Software, Inc. (VSI) is pleased to introduce VSI TCP/IP Services for OpenVMS Alpha V6.0-24, VSI TCP/IP Services for OpenVMS Integrity V6.0-24 and VSI TCP/IP Services for OpenVMS x86-64 V6.0-24.

These products (referred to as VSI TCP/IP Services V6.0 later on in this document) is 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, as well as 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
- Remote (R) Commands
- SMTP

¹VSI 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.

- 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 in VSI TCP/IP Services for OpenVMS 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 SYSS\$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 for OpenVMS V6.0. 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.

2.3. 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
$
```

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. 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.

2.6. SS\$_BADIRECTORY Error when Deleting a File

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

2.7. 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.

2.8. Stale File Reports in OPCOM with NFS Delete Requests

A stale file is occasionally reported by OPCOM, usually with an NFS client delete request.

2.9. NFS Server WRITE Error and Occasional Client Request Issue

Some NFS servers report a WRITE error with the NFS client. On rare occasions, the client sends a request with a bad stability option value.

2.10. 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 previously, refer to *VSI TCP/IP Services for OpenVMS V6.0-23 Release Notes* [<https://docs.vmssoftware.com/vsi-tcpip-services-for-openvms-6023-release-notes/>].

3.1. TCPIP\$CONFIG Fails In Extended Parse Mode

TCPIP\$CONFIG no longer fails in the extended parse mode when a user attempts to configure interfaces from the VSI TCP/IP Services Configuration Menu.

Previously, it would fail with the following error:

```
%DCL-W-IVCHAR, invalid numeric value - check for invalid digits
```

3.2. DNFS Client Handling of Servers That Do Not Support REaddirPLUS

If a server does not support the REaddirPLUS operation or does not return the file attributes, the DNFS client automatically switches from using REaddirPLUS to using the basic REaddir operation followed by the LOOKUP operation. This ensures that the correct set of file attributes is cached.

The switch stays in effect until the DNFS device is dismantled.

3.3. DNFS Client Handling of Return Codes From Certain Functions

Previously, the DNFS client handled the return codes from certain internal functions and QIO operations incorrectly, which could potentially lead to an incorrect path of execution and crash the DNFSACP process.

This issue has been fixed in the current release.

3.4. DNFS Client Fails to Serialize Access to State Data

Previously, under certain conditions, the DNFS client could fail to serialize access to the state data, which would cause the NFSACP process to crash.

This issue has been fixed in the current release.

3.5. DNFS Client Handling of Long File Handles

Previously, the DNFS client incorrectly processed the file handles that were over 32 bytes long. This issue has been fixed in the current release.

3.6. DNFS Client Handling of Odd-Sized File Handles

Previously, the DNFS client failed to correctly encode the server requests where the file handle size was *not* a multiple of 4. This resulted in incorrect parsing of the subsequent fields.

This issue has been fixed in the current release.

3.7. DNFS Client Handling Failed Memory Allocations

Previously, the DNFS client incorrectly handled failed memory allocations, especially when processing the UNSTABLE WRITE operations, potentially leading to a DNFSACP crash.

This issue has been fixed in the current 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 V6.0 TCP/IP Services.
2. If you are currently using the DHCP client, disable it. The DHCP client implementation in V6.0 TCP/IP Services 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 included as part of the VSI OpenSSH product, rather than TCP/IP Services.

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

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)
```

