z/OS V2R4 Communications Server IBM Health Checker for use of native TLS/SSL support for DCAS, FTP server, and TN3270 server

Contents

Chapter 1

New Function Summary

Topics:

IBM Health Checker for use of native TLS/SSL support for DCAS

z/OS® V2R4 Communications Server, with TCP/IP APAR PH16144 and SNA APAR OA58255, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if DCAS uses native TLS/SSL support.

Dependency: You must install TCP/IP APAR PH16144 and SNA APAR OA58255 and start the IBM Health Checker for z/OS to use the new migration health check.

Using the IBM Health Checker for use for native TLS/SSL support for DCAS

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 1: IBM Health Checker for use of native TLS/SSL support for DCAS on page 6.

Table 1: IBM Health Checker for use of native TLS/SSL support for DCAS

Task/Procedure	Reference
To use the new migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL migration health check. 3. Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM® Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for DCAS, see Table 2: All related topics about IBM Health Checker for use of native TLS/SSL support for DCAS on page 6.

Table 2: All related topics about IBM Health Checker for use of native TLS/SSL support for DCAS

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL
z/OS Migration	*IP Services: Migrate TLS/SSL support for DCAS to AT-TLS*
z/OS Communications Server: SNA Messages	• ISTM043I • ISTM044E

IBM Health Checker for use of native TLS/SSL support for the FTP server

z/OS V2R4 Communications Server, with TCP/IP APAR PH21573 and SNA APAR OA59022, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies active FTP servers using native TLS/SSL support.

z/OS V2R4 Communications Server, with TCP/IP APAR PH24732 and SNA APAR OA59490, provides additional migration health checks to use with the IBM Health Checker for z/OS function. These migration health checks identify FTP servers and clients that are configured with an invalid configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS.

Dependencies:

- You must install TCP/IP APAR PH21573 and SNA APAR OA59022 and start the IBM Health Checker for z/OS to use the new migration health check to identify active FTP servers using native TLS/SSL support.
- You must install TCP/IP APAR PH24732 and SNA APAR OA59490 and start the IBM Health Checker for z/OS to use the new migration health checks to identify FTP servers and clients that are configured with an invalid configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS.

Using the IBM Health Checker for use of native TLS/SSL support for the FTP server.

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 3: IBM Health Checker for use of native TLS/SSL support for the FTP server on page 7.

Table 3: IBM Health Checker for use of native TLS/SSL support for the FTP server

Task/Procedure	Reference
To use the new migration health check, take the following steps: **1.** Configure and start the IBM Health Checker for z/OS. **2.** Activate the ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL FTP server migration health check. **3.** Activate the ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL FTP server migration health check. **4.** Activate the ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL FTP client migration health check. **5.** Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for the FTP server, see Table 4: All related topics about IBM Health Checker for use of native TLS/SSL support for the FTP server on page 7.

Table 4: All related topics about IBM Health Checker for use of native TLS/SSL support for the FTP server

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
z/OS Communications Server: IP Configuration Guide	• Steps for customizing the FTP server for TLS • Steps for migrating the FTP server and client to use AT-TLS
IBM Health Checker for z/OS: User's Guide	• ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL • ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL • ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL

Book name	Topics
z/OS Migration	• *IP Services: Migrate TLS/SSL support for FTP server to AT-TLS* • *IP Services: Ensure FTP servers and FTP clients are not configured with TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS*
z/OS Communications Server: SNA Messages	• ISTM045I • ISTM046E • ISTM047I • ISTM048E • ISTM049I • ISTM050E
z/OS Communications Server: IP Messages Volume 3 (EZY)	• EZYFT79I • EZYFT88I

IBM Health Checker for use of native TLS/SSL support for the TN3270 server

z/OS V2R4 Communications Server, with TCP/IP APAR PH16144 and SNA APAR OA58255, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies active TN3270 servers using native TLS/SSL support.

Dependency: You must install TCP/IP APAR PH16144 and SNA APAR OA58255 and start the IBM Health Checker for z/OS to use the new migration health check.

Using the IBM Health Checker for use for native TLS/SSL support for the TN3270 server

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 5: IBM Health Checker for use of native TLS/SSL support for the TN3270 server on page 8.

Table 5: IBM Health Checker for use of native TLS/SSL support for the TN3270 server

Task/Procedure	Reference
To use the new migration health check, take the following steps: **1.** Configure and start the IBM Health Checker for z/OS. **2.** Activate the ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL migration health check. **3.** Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for the TN3270 server, see Table 6: All related topics about IBM Health Checker for use of native TLS/SSL support for the TN3270 server on page 9.

Table 6: All related topics about IBM Health Checker for use of native TLS/SSL support for the TN3270 server

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL
z/OS Migration	*IP Services: Migrate TLS/SSL support for TN3270 to AT-TLS*
z/OS Communications Server: SNA Messages	• ISTM041I • ISTM042E

Chapter 2

IBM Health Checker for z/OS User's Guide

Topics:

ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL

Description:

Checks whether the Digital Certificate Access Server (DCAS) is using native TLS/SSL support. Support for native TLS/SSL support for DCAS will be withdrawn in a future release of IBM z/OS Communications Server.

When this check is active, if it determines that DCAS has TLSMECHANISM DCAS configured, the check will trigger an exception and an entry will be added to the report produced by this check.

Reason for check:

Because native TLS/SSL for DCAS will no longer be supported in a future release of z/OS Communications Server, IBM suggests that customers who currently use or plan to use native TLS/SSL for DCAS, migrate to AT-TLS for DCAS.

z/OS releases the check applies to:

z/OS V2R3 and V2R4.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line (ADDREPLACE POLICY) and use the UPDATE statement on a MODIFY hzsproc command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)][STATEMENT(name)]
UPDATE
CHECK(IBMCS,ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL)
DATE('date_of_the_change')
REASON('Your reason for making the update.')
INACTIVE
SEVERITY(LOW)
INTERVAL(ONETIME)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

For more information on using AT-TLS support for DCAS, see *Migrating the DCAS server to use AT-TLS policies* in *z/OS Communications Server: IP Configuration Guide*.

Messages:

This check issues the following message:

- ISTM044E

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL

Description:

Checks whether one or more active FTP servers are using native TLS/SSL support. Support for native TLS/SSL support for the FTP server will be withdrawn in a future release of IBM z/OS Communications Server.

When this check is active, if it determines that one or more active FTP servers have EXTENSIONS AUTH_TLS and TLSMECHANISM FTP configured, then the check will trigger an exception and an entry will be added to the report produced by this check.

Reason for check:

Because native TLS/SSL for the FTP server will no longer be supported in a future release of z/OS Communications Server, IBM suggests customers who currently use or plan to use native TLS/SSL for FTP server, migrate to AT-TLS for the FTP server.

z/OS releases the check applies to:

z/OS V2R3 and V2R4.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line(ADDREPLACE POLICY) and use the UPDATE statement on a MODIFY hzsproc command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)][STATEMENT(name)]
UPDATE
CHECK(IBMCS,ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL)
DATE('date_of_the_change')
REASON('Your reason for making the update.')
INACTIVE
SEVERITY(LOW)
INTERVAL(ONETIME)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

For more information on using AT-TLS support for the FTP server, see *Steps for migrating the FTP server and client to use AT-TLS* in *z/OS Communications Server: IP Configuration Guide*.

Messages:

This check issues the following message:

- ISTM046E

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL

Description:

Checks whether one or more active FTP clients are configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and SECURE_MECHANISM TLS. This combination is invalid and will be rejected in a future release of IBM z/OS Communications Server.

When this check is active, if it determines one or more active FTP clients have TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS configured, then the check will trigger an exception and will continue to be reported for the duration of the IPL. The message ISTM050E is issued and is followed by message ISTM900I which indicates the date and time that an FTP client with the configuration was last detected. Message EZYFT79I will be issued to syslogd to further assist in determining which FTP client triggered the exception. EZYFT79I messages are written using syslogd facility local1 and priority warning.

Reason for check:

Because the combination of TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS will be rejected in a future release of z/OS Communications Server, IBM suggests customers who currently use this invalid combination, update their configuration to TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005.

z/OS releases the check applies to:

z/OS V2R3 and V2R4 with PTFs for APARs PH24732 and OA59490 applied.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line(ADDREPLACE POLICY) and use the UPDATE statement on a MODIFY hzsproc command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)][STATEMENT(name)]
UPDATE
CHECK(IBMCS,ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL)
DATE('date_of_the_change')
REASON('Your reason for making the update.')
INACTIVE
SEVERITY(LOW)
INTERVAL(24:00)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

See in *z/OS Communications Server: IP Configuration Reference* for additional information about the TLSRFCLEVEL parameter.

Messages:

This check issues the following message:

- ISTM050E

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL

Description:

Checks whether one or more active FTP servers are configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and EXTENSIONS AUTH_TLS. This combination is invalid and will be rejected in a future release of IBM z/OS Communications Server.

When this check is active, if it determines one or more active FTP servers have TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS configured, then the check will trigger an exception and an entry will be added to the report produced by the check.

Reason for check:

Because the combination of TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS will be rejected in a future release of z/OS Communications Server, IBM suggests customers who currently use this invalid combination, update their configuration to TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005.

z/OS releases the check applies to:

z/OS V2R3 and V2R4 with PTFs for APARs PH24732 and OA59490 applied.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line(ADDREPLACE POLICY) and use the UPDATE statement on a MODIFY hzsproc command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)][STATEMENT(name)]
UPDATE
CHECK(IBMCS,ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL)
DATE('date_of_the_change')
REASON('Your reason for making the update.')
INACTIVE
SEVERITY(LOW)
INTERVAL(ONETIME)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

See in *z/OS Communications Server: IP Configuration Reference* for additional information about the TLSRFCLEVEL parameter.

Messages:

This check issues the following message:

- ISTM048E

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL

Description:

Checks whether one or more active TN3270 servers are using native TLS/SSL support. Support for native TLS/SSL support for the TN3270 server will be withdrawn in a future release of IBM z/OS Communications Server.

When this check is active, if it determines that one or more active TN3270 servers have SECUREPORT configured, the check will trigger an exception and an entry will be added to the report produced by this check.

Reason for check:

Because native TLS/SSL for the TN3270 server will no longer be supported in a future release of z/OS Communications Server, IBM suggests that customers who currently use or plan to use native TLS/SSL for TN3270 server, migrate to AT-TLS for the TN3270 server.

z/OS releases the check applies to:

z/OS V2R3 and V2R4.

User override of IBM values:

The following sample shows the defaults for customizable values for this check. Use this sample to make permanent check customizations in an HZSPRMxx parmlib member used at IBM Health Checker for z/OS startup. If you just want a one-time only update to the check defaults, omit the first line (ADDREPLACE POLICY) and use the UPDATE statement on a MODIFY hzsproc command. Note that using non-POLICY UPDATEs in HZSPRMxx can lead to unexpected results and is therefore not recommended.

```
ADDREPLACE POLICY[(policyname)][STATEMENT(name)]
UPDATE
CHECK(IBMCS,ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL)
DATE('date_of_the_change')
REASON('Your reason for making the update.')
INACTIVE
SEVERITY(LOW)
INTERVAL(ONETIME)
```

Debug support:

No

Verbose support:

No

Parameters accepted:

No

Reference:

For more information on using AT-TLS support for the TN3270 server, see *Converting Telnet profile statements to equivalent AT-TLS policy statements* in *z/OS Communications Server: IP Configuration Guide*.

Messages:

This check issues the following message:

- ISTM042E

See *z/OS Communications Server: SNA Messages*.

SECLABEL recommended for multilevel security users:

SYSLOW - see *z/OS Planning for Multilevel Security and the Common Criteria* for information on using SECLABELs.

Chapter 3

z/OS Migration

Topics:

IP Services: Ensure FTP servers and FTP clients are not configured with TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS

Description

The FTP TLSRFCLEVEL CCCNONOTIFY parameter is not valid when AT-TLS is used to protect an FTP connection. This combination produces unexpected results.

For an FTP server, configuring TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS will be rejected in a future release of z/OS Communications Server.

For an FTP client, configuring TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and SECURE_MECHANISM TLS will be rejected in a future release of z/OS Communications Server.

If you are using TLSRFCLEVEL CCCNONOTIFY with AT-TLS, migrate your FTP server and client configurations to use TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005.

Table 7: Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R4
Applies to migration from:	z/OS V2R2 and z/OS V2R3.
Timing:	Before installing z/OS V2R4.
Is the migration action required?	No, but recommended because the combination of TLSRFCLEVEL CCCNONOTIFY and AT-TLS protection will be rejected in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	The following migration health checks can help you determine whether you are using TLSRFCLEVEL CCCNONOTIFY with AT-TLS protection: • For the FTP server: ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL • For the FTP client: ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL These checks are available for z/OS V2R4 with APARs PH24732 and OA59490 applied.

Steps to take

Migrate any FTP server and any FTP client using TLSRFCLEVEL CCCNONOTIFY with AT-TLS to either TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005. See *TLSRFCLEVEL (FTP client and server) statement* in *z/OS Communications Server: IP Configuration Reference* for additional information about this parameter.

Reference information

See *TLSRFCLEVEL (FTP client and server) statement* in *z/OS Communications Server: IP Configuration Reference* for additional information about this parameter.

IP Services: Migrate TLS/SSL support for DCAS to AT-TLS

Description

Support for native TLS/SSL support for DCAS will be removed in a future release of IBM z/OS Communications Server. The following configuration parameters and settings will be removed:

- TLSMECHANISM DCAS
- KEYRING
- LDAPPORT
- LDAPSERVER
- SAFKEYRING
- STASHFILE
- TLSV1ONLY
- V3CIPHER

If you are using native TLS/SSL support for DCAS, migrate to use AT-TLS support.

Table 8: Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	The planned removal was announced in IBM United States Software Announcement *IBM z/OS Version 2 Release 4* dated July 23, 2019.
Applies to migration from:	z/OS V2R2 and z/OS V2R3.
Timing:	Before installing z/OS V2R4.
Is the migration action required?	No, but recommended because native TLS/SSL support for DCAS (TLSMECHANISM DCAS) will be removed in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	The following migration health check can help you determine whether you are using native TLS/SSL for DCAS: ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL This check is available for z/OS V2R3 and V2R4 with APARs PH16144 and OA58255 applied.

Steps to take

If the DCAS server is using native TLS/SSL, migrate it to use AT-TLS policies. See *Migrating the DCAS server to use AT-TLS policies* in *z/OS Communications Server: IP Configuration Guide* for necessary steps to migrate DCAS.

Reference information

See *Migrating the DCAS server to use AT-TLS policies* in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Migrate TLS/SSL support for FTP server to AT-TLS

Description

Support for native TLS/SSL support for the FTP server will be removed in a future release of IBM z/OS Communications Server. The following FTP.DATA parameters and settings for the FTP server will be removed:

- TLSMECHANISM FTP
- TLSRFCLEVEL CCCNONOTIFY
- KEYRING
- CIPHERSUITE
- TLSTIMEOUT
- SSLV3

If you are using native TLS/SSL support for the FTP server, migrate to use AT-TLS support.

Note: TLS/SSL support for the FTP client is unchanged.

Table 9: Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	The planned removal was announced in IBM United States Software Announcement "IBM z/OS Version 2 Release 4" dated July 23, 2019.
Applies to migration from:	z/OS V2R2 and z/OS V2R3.
Timing:	Before installing z/OS V2R4.
Is the migration action required?	No, but recommended because native TLS/SSL support for the FTP server is removed in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	The following migration health check can help you determine whether you are using native TLS/SSL for FTP servers: ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL This check is available for z/OS V2R3 and V2R4 with APARs PH21573 and OA59022 applied.

Steps to take

Migrate any FTP server using native TLS/SSL to use AT-TLS policies. For necessary steps to migrate the FTP server, see *Steps for migrating the FTP server and client to use AT-TLS* in *z/OS Communications Server: IP Configuration Guide*.

Reference information

For necessary steps to migrate the FTP server, see *Steps for migrating the FTP server and client to use AT-TLS* in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Migrate TLS/SSL support for TN3270 to AT-TLS

Description

Support for native TLS/SSL support for TN3270 will be removed in a future release of IBM z/OS Communications Server. The following configuration parameters and settings will be removed:

- SECUREPORT
- CLIENTAUTH
- CRLLDAPSERVER
- ENCRYPTION
- KEYRING
- SSLTIMEOUT
- SSLV2
- NOSSLV2
- SSLV3
- NOSSLV3

If you are using native TLS/SSL support for TN3270, migrate to use AT-TLS support.

Table 10: Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	The planned removal was announced in IBM United States Software Announcement *IBM z/OS Version 2 Release 4* dated July 23, 2019.
Applies to migration from:	z/OS V2R2 and z/OS V2R3.
Timing:	Before installing z/OS V2R4.
Is the migration action required?	No, but recommended because native TLS/SSL support for TN3270 will be removed in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Related IBM Health Checker for z/OS check:	The following migration health check can help you determine whether you are using native TLS/SSL for TN3270: ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL This check is available for z/OS V2R3 and V2R4 with APARs PH16144 and OA58255 applied.

Steps to take

If the TN3270 server is using native TLS/SSL, migrate it to use AT-TLS policies. See *Converting Telnet profile statements to equivalent AT-TLS policy statements* in *z/OS Communications Server: IP Configuration Guide* for necessary steps to migrate TN3270.

Reference information

See *Converting Telnet profile statements to equivalent AT-TLS policy statements* in *z/OS Communications Server: IP Configuration Guide*.

Chapter 4

IP Configuration Guide

Topics:

Steps for customizing the FTP server for TLS

You can customize the FTP server for TLS, but a better way to implement TLS security is by using AT-TLS.

Understand the following information:

- The FTP server can be enabled to support both TLS and Kerberos. Some of the configuration statement settings apply to both TLS and Kerberos and affect the behavior of both.
- To support TLS, the FTP server always provides server certificate authentication to all the clients to validate that the server is what it says it is. Therefore, a server key ring database is required to contain at least the FTP server's digital certificate and private key. For more information about key ring databases, see *TLS/SSL security*.
- The FTP server can implement TLS security by itself, or the FTP server can be configured to use Application Transparent Transport Layer Security (AT-TLS) as a controlling application. For more information about AT-TLS, see *Application Transparent Transport Layer Security data protection*.

  Guideline: Using AT-TLS is the better way to implement TLS security. With AT-TLS, for example, you can have the following implementation:

  - Specify the label of the certificate to be used for authentication instead of using the default certificate
  - Support SSL Session Key Refresh
  - Support SSL Sysplex Session ID Caching
  - Trace decrypted SSL data for FTP in a data trace
  - Receive more detailed diagnostic messages in syslogd

  Requirement: AT-TLS requires Policy Agent to be configured, and the TCP/IP stack to be enabled for AT-TLS. To configure AT-TLS, see *Configuring the server system*.

Perform the following steps to customize the FTP server for TLS:

1. Decide what level of RFC 4217, *On Securing FTP with TLS*, that you want the server to support.

   - To have the server support *On Securing FTP with TLS* at the Internet draft level, code the following statement in the server's FTP.DATA configuration file:

     ```
     TLSRFCLEVEL DRAFT
     ```

     This is the default. The z/OS FTP server has supported TLS security at this level since V1R2. Code this statement in FTP.DATA to maintain this level of support.
   - To have the server support *On Securing FTP with TLS* at the RFC 4217 level, code the following statement in the server's FTP.DATA configuration file:

     ```
     TLSRFCLEVEL RFC4217
     ```

     The RFC *On Securing FTP with TLS* was published as RFC 4217 in October, 2005. The RFC differs from the Internet draft in its description of the AUTH, CCC, and REIN commands. RFC 4217 is less restrictive than the Internet draft regarding when the AUTH and CCC commands can be sent to the server, and more explicit about the details of the server REIN implementation. For more information, see RFC 4217.
2. Code the following statement in the server's FTP.DATA configuration file to enable the server for TLS:

   ```
   EXTENSIONS AUTH_TLS
   ```
3. Decide what level of authentication you will use for TLS sessions:

   - Server authentication only
   - Client authentication level 1
   - Client authentication level 2
   - Client authentication level 3

   For more information about server authentication and client authentication, see *Secure Socket Layer overview*.

4. Create the server key ring database and add the certificates you will need to the server key ring database.

   Every TLS session handshake includes server authentication, so you must always add a certificate for this server to the server key ring database. If a server certificate is self signed, you must also export that certificate to the key ring databases of those clients that will log in using TLS. If a server certificate is signed by a certificate authority (CA), the CA certificate used to sign the server certificate needs to be in the client key ring databases, rather than the server certificate. For more information about server authentication, see *Server authentication* .

   If you are using client authentication and self-signed certificates, you must import the client certificates into the server key ring database. If a client certificate is signed by a CA, the CA certificate used to sign the client certificate needs to be in the server key ring database, rather than the client certificate. For more information, see *Client authentication*.

5. Decide whether FTP will implement TLS security or AT-TLS will implement TLS security.

   The default is to have FTP implement TLS security. This setting is customized by using the TLSMECHANISM configuration statement.

   - To configure the FTP server to use AT-TLS for TLS security, code the following statement in FTP.DATA:

     ```
     TLSMECHANISM ATTLS
     ```

   - To configure the FTP server to implement TLS security by itself, code the following statement in FTP.DATA:

     ```
     TLSMECHANISM FTP
     ```

     This is the default setting.

6. If using TLSMECHANISM FTP, you must configure the FTP server with a key ring database.

   To configure the FTP server with the name of the key ring database, code the following statement in FTP.DATA:

   ```
   KEYRING server-keyring-database
   ```

   For information about the KEYRING statement, see z/OS Communications Server: IP Configuration Reference.

7. Decide whether clients logging in to this server should be required to use the TLS protocol.

   The default is to allow the client to decide whether to use TLS. This setting is customized by using the SECURE_FTP configuration statement. You should understand that its setting affects both TLS security behavior and Kerberos security behavior.

   To allow the client to decide whether to use TLS, code the following statement in the server's FTP.DATA configuration file:

   ```
   SECURE_FTP ALLOWED
   ```

   This is the default setting, and indicates:

   - If the server is enabled for TLS only, clients must either log in using TLS, or with no security mechanism.
   - If the server is enabled for Kerberos only, clients must either log in using Kerberos, or with no security mechanism.
   - If the server is enabled for both TLS and Kerberos, clients can log in using TLS, Kerberos, or with no security mechanism.

   To require that clients log in using a security mechanism, code the following statement in the server's FTP.DATA configuration file:

   ```
   SECURE_FTP REQUIRED
   ```

   This setting indicates:

   - If the server is enabled for TLS only, clients must log in using TLS.
   - If the server is enabled for Kerberos only, clients must log in using Kerberos.
   - If the server is enabled for both TLS and Kerberos, clients must log in using either TLS or Kerberos.

8. If you do not want to use client authentication, you can code the following statement in the server's FTP.DATA configuration file:

```
SECURE_LOGIN NO_CLIENT_AUTH
```

This is the default.

If you do want to use client authentication, the following levels of client authentication are possible:

- Level 1 authentication is performed by system SSL. The client passes an X.509 certificate to the server. To pass authentication, the Certificate Authority that signed the client certificate must be considered trusted by the server. To use level 1 client authentication, code the following statement in the server's FTP.DATA configuration file:

  ```
  SECURE_LOGIN REQUIRED
  ```

- Level 2 authentication provides level 1 authentication, and additionally requires that the client certificate be registered with RACF® (or another SAF compliant security product) and mapped to a user ID. The client certificate received during the SSL handshake is used to query the security product to verify that the certificate maps to a user ID known to the system prior to connection negotiation. To use level 2 client authentication, code the following statement in the server's FTP.DATA configuration file:

  ```
  SECURE_LOGIN VERIFY_USER
  ```

- Level 3 authentication provides level 1 and 2 authentication. In addition, it provides the capability to restrict access to the server based on the user ID returned from RACF. If the SERVAUTH class of RACF is active and the server's port profile is defined, a connection is accepted only if the requester's user ID associated with the client certificate is defined in the server's port profile. To use level 3 client authentication, code the following statement in the server's FTP.DATA configuration file:

  ```
  SECURE_LOGIN VERIFY_USER
  ```

  Also, define the server's port profile in the SERVAUTH class of RACF.

If you choose to use client authentication, you can also use the client certificate authentication process to eliminate the client login password prompt so that a client supplies only the login user ID to establish the session. The certificate received from the client must be registered in the security product and must be associated with the login user ID. You can use the RACDCERT ADD command to register and associate the certificate. If either the certificate is not registered or is not associated with the user ID, you will be prompted for a password.

If you do not want to use the client authentication process to eliminate the client password prompt, you can code the following statement in the server's FTP.DATA configuration file:

```
SECURE_PASSWORD REQUIRED
```

This is the default.

If you want to use the client authentication process to eliminate the client password prompt, along with your client authentication statement (either SECURE_LOGIN REQUIRED or SECURE_LOGIN VERIFY_USER), code the following statement in the server's FTP.DATA configuration file:

```
SECURE_PASSWORD OPTIONAL
```

9. If you specified TLSMECHANISM ATTLS, configure the AT-TLS policy for the FTP server.

   To configure AT-TLS, see *Configuring the server system*.

   Requirements:

   - The FTP server is a controlling application. For more information about controlling applications, see *Advanced application considerations*.

     Code a TTLSEnvironmentAdvancedParms statement with the ApplicationControlled and SecondaryMap parameters; both parameters should specify the value On. The ApplicatonControlled parameter allows FTP to start and stop TLS security on a connection. The SecondaryMap parameter enables active or passive data connections to use the AT-TLS policy that is used for the control connection. You do not need to code any additional TTLSRule statements for the data connections.
   - The FTP server requires that the HandshakeRole parameter with the value Server or ServerWithClientAuth be coded on the TTLSEnvironmentAction statement. If the SECURE_LOGIN statement is coded in FTP.DATA with the parameters REQUIRED or VERIFY_USER, the HandshakeRole parameter value must be ServerWithClientAuth.
   - The TTLSRule statement for the FTP server requires the Direction parameter with the value Inbound.

   A sample Policy Agent AT-TLS configuration showing the required policy configuration statements for AT-TLS is as follows:

```
   TTLSGroupAction  secure_ftp_server_group
   {
      TTLSEnabled On
   }
   TTLSEnvironmentAction secure_ftp_server_env
   {
      TTLSKeyringParms
      {
         Keyring server-keyring-database
      }
      HandshakeRole Server       # When Secure_Login NO_CLIENT_AUTH is coded
      #HandshakeRole ServerWithClientAuth # When Secure_Login Required or Verify_User is coded
      TTLSEnvironmentAdvancedParms
      {
         ApplicationControlled On
         SecondaryMap  On
      }
      TTLSCipherParmsRef   ftp_server_ciphers     # Used to customize ciphersuites for the FTP
                                                  # server
   }
TTLSCipherParms ftp_server_ciphers
{
   # Sample ciphers.  Should be customized!
   V3CipherSuites TLS_RSA_WITH_AES_256_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_NULL_SHA
}

   TTLSRule secure_ftp_server_rule
   {
      LocalPortRange 21                  # This should be set to the port the FTP server is
                                         #  listening on
      Direction Inbound
      TTLSGroupActionRef secure_ftp_server_group
      TTLSEnvironmentActionRef secure_ftp_server_env
   }
```

   Tip: You can enable additional security settings with AT-TLS, such as LDAP servers and handshake timeout values. The configuration used in the example is the minimum required to allow the FTP server to use AT-TLS. You can add additional configuration statements.

10. Decide which cipher algorithms the server should use to encipher data transfers and to encipher control information.

    FTP and AT-TLS support TLS through the system SSL cryptographic services base element of z/OS. System SSL supports multiple cipher algorithms that provide both encryption and data authentication (that is, data integrity). Encryption scrambles the data so it is transferred confidentially and cannot be interpreted without a special key. Data authentication algorithms ensure the data was not modified during transfer. Some of the supplied cipher algorithms provide only data authentication, and some provide both encryption and authentication. Be aware that the actual cipher algorithm used for the session is determined by a negotiation between the server and client. For example, if you configure an FTP server to use the Triple DES encryption, SHA authentication algorithm, but

the client does not support that cipher algorithm, Triple DES encryption, SHA authentication will not be used for sessions between the server and that client.

If using TLSMECHANISM FTP, select which cipher algorithms you prefer to use by coding a CIPHERSUITE configuration statement in the FTP.DATA file for each cipher algorithm the server can use. For a list of the cipher algorithms you can specify on the CIPHERSUITE statement, see z/OS Communications Server: IP Configuration Reference. List the CIPHERSUITE statements in FTP.DATA in the order of preference, your most preferred cipher algorithm being first. System SSL will negotiate a cipher algorithm with the server on behalf of the client using the same order of preference as is indicated by the order of CIPHERSUITE statements in FTP.DATA.

If you specify TLSMECHANISM ATTLS, select which cipher algorithms you want to use by coding a TTLSCipherParms configuration statement to specify the cipher algorithms that the server can use. For a list of the cipher algorithms you can specify with the TTLSCipherParms statement, see z/OS Communications Server: IP Configuration Reference. List the ciphers in the order of preference, your most preferred cipher algorithm first. The cipher algorithm is negotiated with the server on behalf of the client using the same order of preference as indicated by the order of the TTLSCipherParms statement.

Restrictions:

- Only RSA key exchange is supported.
- The following algorithms are subject to export regulations and might not be available to your system:
  - Triple DES encryption, SHA authentication
  - RC4 (128-bit) encryption, SHA authentication
  - RC4 (128-bit) encryption, MD5 authentication
  - AES (128-bit and 256-bit) encryption, SHA authentication

11. Decide the level of security for the data connection.

You can choose to require enciphered data transfers, or to allow the client to decide the level of security for data transfers. The default is to allow the clients to decide the level of security.

This setting is customized by using the SECURE_DATACONN configuration statement. You should understand that its setting affects both TLS security behavior and Kerberos security behavior.

If you want the server to require that data is transferred raw with no cipher algorithm applied to the data and that clients attempting to use ciphers are rejected, code the following statement in the server's FTP.DATA configuration file:

```
SECURE_DATACONN NEVER
```

If you want the client to decide whether data is transferred raw or enciphered, you can code the following statement in the server's FTP.DATA configuration file:

```
SECURE_DATACONN CLEAR
```

This is the default.

For TLS, the client decides whether data is enciphered or not. If it indicates it should be enciphered, the cipher algorithm is negotiated between the server and the client using TLS protocols. For Kerberos, the client can specify whether data is transferred raw, integrity protected only, or both integrity and privacy protected.

If you want the server to require that data is transferred enciphered and that clients attempting to send raw data are rejected, code the following statement in the server's FTP.DATA configuration file:

```
SECURE_DATACONN PRIVATE
```

For TLS, the cipher algorithm is negotiated between the server and the client using TLS protocols. For Kerberos, the data must be transferred using both integrity and privacy protection. Clients attempting to send data that is only integrity protected are rejected.

12. Decide whether the server requires session reuse when SSL/TLS is used to protect the control and data connections.

    By default, the server is enabled to reuse either of the following SSL session IDs on the data connections within an FTP session:

    - The SSL session ID of the control connection
    - The SSL session ID of a previous data connection

    This setting is customized by using the SECURE_SESSION_REUSE configuration statement.

    - To enable the server to reuse either of the following SSL session IDs on the subsequent data connections within an FTP session, code ALLOWED on the SECURE_SESSION_REUSE statement in the FTP.DATA configuration file of the server:

      - The SSL session ID of the control connection
      - The SSL session ID of a previous data connection

      This is the default.
    - To require the server to reuse the SSL session ID of the control connection on the subsequent data connections within an FTP session, code REQUIRED on the SECURE_SESSION_REUSE statement in the FTP.DATA configuration file of the server.

      This setting might cause data connections and FTP transfers to fail when the remote side does not support reusing the session ID.

    For information about the SECURE_SESSION_REUSE statement, see z/OS Communications Server: IP Configuration Reference.
13. For information about configuring your security product for TLS, see *TLS/SSL security* in *z/OS Communications Server: IP Configuration Guide*.

Steps for migrating the FTP server and client to use AT-TLS

Application Transparent Transport Layer Security (AT-TLS) is the best way to implement TLS security for the FTP server and client. AT-TLS provides additional functionality and performance for TLS secured connections.

Perform the following steps to migrate from an existing configuration using TLS security for the FTP server and client to a configuration using AT-TLS:

1. Configure AT-TLS and Policy Agent.

   For details about AT-TLS setup, see *Application Transparent Transport Layer Security data protection*. For Policy Agent setup and AT-TLS policy statements, see z/OS Communications Server: IP Configuration Reference.

   Requirements:

   - The FTP server and client are controlling applications. For more information about controlling applications, see *Advanced application considerations*.

     Code a TTLSEnvironmentAdvancedParms statement with the ApplicationControlled and SecondaryMap parameters; both parameters should specify the value On. The ApplicatonControlled parameter allows FTP to start and stop TLS security on a connection. The SecondaryMap parameter enables active or passive data connections to use the AT-TLS policy that is used for the control connection. You do not need to code any additional TTLSRule statements for the data connections.
   - The FTP server requires the HandshakeRole parameter with the value Server or ServerWithClientAuth to be coded on the TTLSEnvironmentAction statement. If the SECURE_LOGIN statement is coded in

FTP.DATA with the parameters REQUIRED or VERIFY_USER, the HandshakeRole parameter value must be ServerWithClientAuth.

- The TTLSRule statement for the FTP server requires the Direction parameter with the value Inbound.
- The FTP client requires the HandshakeRole parameter with the value Client to be coded on the TTLSEnvironmentAction statement.
- The TTLSRule statement for the FTP client requires the Direction parameter with the value Outbound.

Guideline: The FTP server and client do not support SSLv2 when using TLSMECHANISM FTP. By default, AT-TLS does not enable SSLv2. SSLv2 should not be enabled in AT-TLS unless explicitly required by a remote system. If SSLv2 is required by a remote system, use a specific TTLSRule statement for the remote system that points to a TTLSConnectionAction statement enabling SSLv2.

2. Configure the FTP server and client to use AT-TLS by coding TLSMECHANISM ATTLS in FTP.DATA.
3. If TLSRFCLEVEL CCCNONOTIFY is configured in FTP.DATA, update TLSRFCLEVEL to have a valid value for AT-TLS.
4. Use Table 11: Migrating existing FTP server and client configuration on page 32 to migrate the existing FTP server and client configuration to AT-TLS.

   Remove the statements from FTP.DATA and code the AT-TLS equivalent statement.

Table 11: Migrating existing FTP server and client configuration

FTP.DATA statement	AT-TLS equivalent statement	AT-TLS policy statement
KEYRING	Keyring	TTLSKeyRingParms -> TTLSEnvironmentAction
CIPHERSUITE	V3CipherSuites	TTLSCipherParms -> TTLSEnvironmentAction or TTLSConnectionAction
TLSTIMEOUT	GSK_V3_SESSION_TIMEOUT	TTLSGskAdvancedParms -> TTLSEnvironmentAction
SSLV3	SSLv3	TTLSEnvironmentAdvancedParms-> TTLSEnvironmentAction Or TTLSConnectionAdvancedParms-> TTLSConnectionAction

5. Use Table 12: Migrating existing ciphers on page 32 to migrate existing ciphers coded on CIPHERSUITE statements in FTP.DATA to AT-TLS TTLSCipherParms statements.

Table 12: Migrating existing ciphers

CIPHERSUITE cipher	V3CipherSuites cipher	Hexadecimal value
SSL_DES_SHA	TLS_RSA_WITH_DES_CBC_SHA	09
SSL_3DES_SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	0A
SSL_NULL_MD5	TLS_RSA_WITH_NULL_MD5	01
SSL_NULL_SHA	TLS_RSA_WITH_NULL_SHA	02
SSL_RC2_MD5_EX	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	06
SSL_RC4_MD5	TLS_RSA_WITH_RC4_128_MD5	04
SSL_RC4_MD5_EX	TLS_RSA_EXPORT_WITH_RC4_40_MD5	03
SSL_AES_128_SHA	TLS_RSA_WITH_AES_128_CBC_SHA	2F

CIPHERSUITE cipher	V3CipherSuites cipher	Hexadecimal value
SSL_AES_256_SHA	TLS_RSA_WITH_AES_256_CBC_SHA	35

For example, for an FTP.DATA file that contains the following statements:

```
CIPHERSUITE SSL_AES_256_SHA
CIPHERSUITE SSL_3DES_SHA
CIPHERSUITE SSL_NUL_SHA
```

The equivalent TTLSCipherParms statement:

```
TTLSCipherParms
{
   V3CipherSuites TLS_RSA_WITH_AES_256_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_NULL_SHA
}
```

6. AT-TLS supports more secure TLS versions and ciphers. Consider enabling TLSv1.2 or TLSv1.3 on the TTLSEnvironmentAdvancedParms or TTLSConnectionAdvancedParms statement. Consider enabling support for additional ciphers on the TTLSCipherParms statement.

Chapter 5

IP Diagnosis Guide

Topics:

IBM Health Checker for z/OS

IBM Health Checker for z/OS is a z/OS component that installations can use to gather information about their system environment and system parameters to help identify potential configuration problems before they impact availability or cause outages. Individual products, z/OS components, or ISV software can provide checks that take advantage of the IBM Health Checker for z/OS framework.

For more information about IBM Health Checker for z/OS, see IBM Health Checker for z/OS: User's Guide.

z/OS Communications Server TCP/IP provides the following checks:

CSAPP_FTPD_ANONYMOUS_JES	Checks whether the following statements have been configured for an FTP server: • ANONYMOUS • ANONYMOUSLEVEL 3 • ANONYMOUSFILETYPEJES FALSE When ANONYMOUS FTP is allowed on the FTP server, it is recommended that the value specified for ANONYMOUSLEVEL be 3 and that the value specified for ANONYMOUSFILETYPEJES be FALSE. Otherwise, anonymous users can submit jobs to run on the system.
CSAPP_MVRSHD_RHOSTS_DATA	Checks whether the MVRSHD server is active and if an RSH client has been detected using RHOSTS.DATA datasets for authentication. The MVRSHD server supports the RSH and REXEC protocols which transfer user ID and password information in the clear. There is also the potential of weak authentication for RSH clients that use RHOSTS.DATA datasets. This authentication method allows remote command execution without requiring the RSH client to supply a password.
CSAPP_SNMPAGENT_PUBLIC_COMMUNITY	Checks whether the SNMP agent has been configured with a community name of public. The community name of public is a well-known name and should not be used with community-based security due to security considerations.
CSRES_AUTOQ_GLOBALTCPIPDATA	Checks whether the AUTOQUIESCE operand has been specified on the UNRESPONSIVETHRESHOLD resolver setup statement and that the GLOBALTCPIPDATA resolver setup statement has not been specified in the resolver setup file.
CSRES_AUTOQ_RESOLVEVIA	Checks whether the RESOLVEVIA statement has been specified with the value TCP in the global TCPIP.DATA file when the autonomic quiescing of unresponsive name servers function is active.
CSRES_AUTOQ_TIMEOUT	Checks whether the configured resolver timeout value in the global TCPIP.DATA file exceeds the optimal setting when the autonomic quiescing of unresponsive name servers function is active. By default, this check is performed once when the resolver is initialized and whenever a MODIFY REFRESH command is issued. This default value can be overridden on either a POLICY

statement in the HZSPRM*xx* parmlib member or on a MODIFY command.

CSTCP_CINET_PORTRNG_RSV_*TCPIPstackname* Checks whether the port range specified by INADDRANYPORT and INADDRANYCOUNT in the BPXPRMxx parmlib member is reserved for OMVS on this stack, when operating in a CINET environment. A port range is reserved on a TCP/IP stack using the PORTRANGE TCP/IP profile statement. By default, this check is performed once at stack initialization. This default can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by *TCPIPstackname*, which is the job name of each TCP/IP stack that is started, to define a separate check for each stack.

CSTCP_IPMAXRT4_*TCPIPstackname* Checks whether the total number of IPv4 indirect routes in the TCP/IP stack routing table has exceeded the maximum threshold. When this threshold is exceeded, OMPROUTE and the TCP/IP stack can potentially experience high CPU consumption from routing changes. A large routing table is considered to be inefficient in network design and operation. By default, this check is performed at the following times:

- Whenever the total number of indirect routes exceeds the maximum threshold (default 2000)
- 30 minutes after stack initialization (provided that the maximum threshold has not been exceeded)
- Specified interval (default 168 hours for weekly)

The defaults for the maximum threshold and interval can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by *TCPIPstackname*, which is the job name of each TCP/IP stack that is started, to define a separate check for each stack.

CSTCP_IPMAXRT6_*TCPIPstackname* Checks whether the total number of IPv6 indirect routes in the TCP/IP stack routing table has exceeded the maximum threshold. When this threshold is exceeded, OMPROUTE and the TCP/IP stack can potentially experience high CPU consumption from routing changes. A large routing table is considered to be inefficient in network design and operation. By default, this check is performed at the following times:

- Whenever the total number of indirect routes exceeds the maximum threshold (default 2000)
- 30 minutes after stack initialization (provided that the maximum threshold has not been exceeded)
- Specified interval (default 168 hours for weekly)

The defaults for the maximum threshold and interval can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by

	TCPIPstackname, which is the job name of each TCP/IP stack that is started, to define a separate check for each stack.
CSTCP_IWQ_IPSEC_TCPIP*stackname*	Checks whether a QDIO interface defined on a TCP/IP stack has support for inbound workload queueing (IWQ) of IPSec traffic (this is supported by OSA-Express6S and beyond), and whether the TCP/IP stack is configured to have IPSec enabled. If these conditions are met, an additional ancillary input queue (AIQ) is established for IPSec inbound traffic. Each AIQ increases fixed storage utilization. It should be ensured that there is sufficient fixed storage for the AIQ for IPSec traffic. See IP services: Ensure storage availability for IWQ IPSec traffic in z/OS Migration for information on how much storage is needed for IWQ for IPSec. By default, this check will be performed once at stack initialization. The check name is suffixed by TCPIP*stackname*, which is the job name of each TCP/IP stack that is started, to define a separate check for each stack.
CSTCP_SYSTCPIP_CTRACE_*TCPIPstackname*	Checks whether TCP/IP Event Trace (SYSTCPIP) is active with options other than the default options (MINIMUM, INIT, OPCMDS, or OPMSGS). By default, this check will be performed once at stack initialization and then will be repeated once every 24 hours. This default can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by *TCPIPstackname*, which is the job name of each TCP stack that is started, to define a separate check for each stack.
CSTCP_SYSPLEXMON_RECOV_*TCPIPstackname*	Checks whether the IPCONFIG DYNAMICXCF or IPCONFIG6 DYNAMICXCF parameters have been specified and the GLOBALCONFIG SYSPLEXMONITOR RECOVERY parameter has been specified. This check produces an exception message if the IPCONFIG DYNAMICXCF or IPCONFIG6 DYNAMICXCF parameters were specified, but the GLOBALCONFIG SYSPLEXMONITOR NORECOVERY parameter is in effect. By default, this check is performed once at stack initialization. This default can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by *TCPIPstackname*, which is the job name of each TCP stack that is started, to define a separate check for each stack.
CSTCP_TCPMAXRCVBUFRSIZE_*TCPIPstackname*	Checks whether the configured TCP maximum receive buffer size is sufficient to provide optimal support to the z/OS Communications Server FTP Server. By default, this check is performed once at stack initialization and whenever a VARY TCPIP,,OBEYFILE command changes the TCPMAXRCVBUFRSIZE parameter. By

	default, it checks that TCPMAXRCVBUFRSIZE is at least 180K. These defaults can be overridden on either a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. The check name is suffixed by *TCPIPstackname*, which is the job name of each TCP stack that is started, to define a separate check for each stack.
ZOSMIGV2R4PREV_CS_IWQSC_TCPIP*stackname*	This is a migration health check. It checks whether the TCP/IP stack has IWQ and IPSec enabled, and whether any of the QDIO interfaces configured on the stack do not support IWQ IPSec. If IWQ and IPSec are enabled, but a QDIO interface does not support IWQ IPSec, then this check will trigger an exception. In case of migration to an OSA-Express6S, IWQ IPSec support will automatically turn on, and an additional ancillary input queue (AIQ) will be established for IPSec inbound traffic. Each AIQ increases fixed storage utilization. It should be ensured that there is sufficient fixed storage for the AIQ for IPSec traffic. See IP services: Ensure storage availability for IWQ IPSec traffic in z/OS Migration for information on how much storage is needed for IWQ for IPSec. The check name is suffixed by TCPIP*stackname*, which is the job name of each TCP/IP stack that is started, to define a separate check for each stack.
ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL	Checks whether native TLS/SSL support is in use for Digital Certificate Access Server (DCAS). By default, this check is inactive. This default can be overridden on a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. If an IBM Health Checker for z/OS exception message is generated, migration must be performed.
ZOSMIG2R4_NEXT_CS_FTPSRV_NTVSSL	Checks whether native TLS/SSL support is in use for any active FTP servers. By default, this check is inactive. This default can be overridden on a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. If an IBM Health Checker for z/OS exception message is generated, migration must be performed.
ZOSMIG2R4_NEXT_CS_FTPSRV_RFCLVL	Checks whether one or more active FTP servers are configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and EXTENSIONS AUTH_TLS. By default, this check is inactive. This default can be overridden on a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. If an IBM Health Checker for z/OS exception message is generated, migration must be performed.
ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL	Checks whether one or more active FTP clients are configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and SECURE_MECHANISM TLS. By default, this check is inactive. This default can be overridden on a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. If an IBM Health Checker for z/

	OS exception message is generated, migration must be performed.
ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL	Checks whether native TLS/SSL support is in use for any active TN3270 servers. By default, this check is inactive. This default can be overridden on a POLICY statement in the HZSPRMxx parmlib member or on a MODIFY command. If an IBM Health Checker for z/OS exception message is generated, migration must be performed.

Chapter 6

IP Messages: Volume 3 (EZY)

Topics:

EZYFT79I

TLSRFCLEVEL CCCNONOTIFY is not valid with ATTLS for the FTP client: Userid *userid* Jobname *jobname* Local site configuration *local_path*

Explanation

TLSRFCLEVEL CCCNONTIFY has been configured with SECURE_MECHANISM TLS and TLSMECHANISM ATTLS for the FTP client. This combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server. See z/OS Communications Server: IP Configuration Reference for information on the TLSRFCLEVEL parameter.

In the message text:

jobname
The job name of the FTP client

userid
The user id of the FTP client

local_path

LOCSITE COMMAND

If the TLSRFCLEVEL was changed to CCCNONOTIFY for an FTP client using the LOCSITE command, *local_path* will indicate `LOCSITE COMMAND`.

name of FTP client configuration file

If TLSRFCLEVEL CCCNONOTIFY is configured in FTP.DATA for the FTP client, *local_path* indicates which FTP.DATA file is being used. *local_path* will either be `DD:SYSFTPD`, indicating that the SYSFTP DD statement was used for the FTP.DATA file, or it will be the actual name of the file being used. See z/OS Communications Server: IP Configuration Reference for information about the FTP.DATA file search order.

System action

Processing continues with the current configuration.

Operator response

Contact the system programmer.

System programmer response

The configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and SECURE_MECHANISM TLS will be rejected in a future release of z/OS Communications Server. The configuration for this FTP client should be updated to specify TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005.

User response

Not applicable.

Problem determination

See the System Programmer Response.

Module

EZAFTPEP

Routing code

10

Descriptor code

12

Automation

Not applicable for automation.

Example

```
EZYFT79I TLSRFCLEVEL CCCNONOTIFY is not valid with ATTLS for the FTP client:
 Userid USER13 Jobname FTPGET Local site configuration /etc/ftp.data
```

EZYFT88I

Both TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS were specified. This combination produces unexpected results.

Explanation

TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS has been configured for the FTP server. The combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server. See z/OS Communications Server: IP Configuration Reference for information on the TLSRFCLEVEL parameter.

System action

Processing continues with the current configuration.

Operator response

Contact the system programmer.

System programmer response

The configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS will be rejected in a future release of z/OS Communications Server. Update the FTP server configuration to specify TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005.

User response

Not applicable.

Problem determination

See the System Programmer Response.

Module

EZAFTPDM

Routing code

10

Descriptor code

12

Automation

Not applicable for automation.

Example

Not applicable

Chapter 7

IP Messages: Volume 4 (EZZ, SNM)

Topics:

EZZ6035I

jobname DEBUG *type level*

Explanation

A diagnostic message was displayed for debugging purposes.

In the message text:

jobname

The name of the procedure that is used to start the TN3270 server or the job name identifier of the procedure that is used to start the TN3270 server.

If you start the TN3270.TNSRV1 server, the *jobname* value TNSRV1. If you start the TN3270 server, the *jobname* value is TN3270

type* and *level

The *type* value and the *level* value can be one of the following combinations.

- If the *type* value is CONN, the *level* value will be one of the following.
  - EXCEPTION or DETAIL

```
EZZ6035I jobname DEBUG CONN   level
IP..PORT: ipaddr..port
CONN: connid   LU: luname  MOD: modname
RCODE: rcode-instance  description
PARM1: parm  PARM2: parm  PARM3: parm
```

  - TRACE

```
EZZ6035I jobname DEBUG CONN   TRACE
IP..PORT: ipaddr..port
CONN: connid   LU: luname  MOD: modname
    dir     tracedata
PARM1: parm  PARM2: parm  PARM3: parm
```

- If the *type* value is TASK, the *level* value will be the following.
  - EXCEPTION or DETAIL

```
EZZ6035I jobname DEBUG TASK   level
TASK: taskname     MOD: modname
RCODE: rcode-instance  description
PARM1: parm  PARM2: parm  PARM3: parm
```

- If the *type* value is CONFIG, the *level* value will be one of the following.
  - EXCEPTION

```
EZZ6035I jobname DEBUG CONFIG EXCEPTION
LINE: line                MOD: modname
RCODE: rcode-instance  description
PARM1: parm  PARM2: parm  PARM3: parm
```

  - TRACE

```
EZZ6035I jobname DEBUG CONFIG TRACE
LINE: line                MOD: modname
  profdata
PARM1: parm  PARM2: parm  PARM3: parm
```

ipaddr..port

The client IP address and port number if appropriate.

connid

The connection ID assigned by the TCPIP stack.

luname

The name of the Telnet LU representing the client.

line

The line number in the profile of the statement generating the message. If the statement includes several lines, such as TELNETPARMS, the line number indicates the first line of the lines that comprise the statement. The *N/A* value indicates that a problem was found after profile processing was complete.

modname

The name of the module reporting the error. For trace entries, this field is used as a source and destination field.

dir

The direction of the data flow.

tracedata

The first 48 bytes of data that was sent or received from the client or the VTAM® application. The request parameter list (RPL) is included, if applicable. If the *tracedata* value is a BIND, the entire BIND is included.

profdata

The *profdata* value can be one of the following:

profstdata

All the parameters following the statement name.

profcbdata

The structured data passed to the Telnet database.

parm

The value for PARM1, PARM2, or PARM3, which provides additional information specific to the message the *type* value and *level* value combination.

- If the *type* value and *level* values are CONN EXCEPTION, CONN DETAIL, TASK EXCEPTION, TASK DETAIL, and CONFIG EXCEPTION, then the *parm* value is specific to the *rcode* value: see the description of the *rcode* value.
- If the *type* value and *level* values are CONN TRACE, then PARM1 is the length, in hexadecimal, of the data being traced. PARM2 and PARM3 are not used.
- If the *type* value and *level* values are CONFIG TRACE of the configuration statement, PARM1 is the number of words following the statement, PARM2 is not used, and PARM3 is the statement itself.
- If the *type* value and *level* values are CONFIG TRACE of the configuration control block, PARM1 is the number of bytes, in hexadecimal, in the structure passed, PARM2 is the Telnet internal code for the statement, and PARM3 is the statement itself.

instance

The instance number of the error in the module.

rcode* and *description

The *rcode* value is the return code and the *description* value is the text of the return code. The code might indicate an error or it might indicate normal processing. The following are the *rcode* and *description* values:

0000 OK

No errors encountered.

0008 Storage obtain request failed.

This might be caused by a low storage condition or by parameters that were not valid being passed on the storage request. Verify storage availability. In some cases, The PARM1 value is the size of the storage request. If storage is available, contact the IBM software support center.

0009 Storage release request failed.

This might be caused by trying to free the same storage more than once or by passing parameters that are not valid on the storage request. If a storage release failure occurs, contact the IBM software support center.

000A IOCTL request failed.

Telnet issues an IOCTL request to update information used by the NETSTAT display command. The PARM1 value is the IOCTL return value, the PARM2 value is the IOCTL return code, and the PARM3 value is the IOCTL reason code. If an IOCTL failure occurs, contact the IBM software support center.

000B Available return code.

This return code is not used and is available for future use.

000C Timer request failed.

Telnet requested a timer and the request failed. Contact the IBM software support center.

000D Lock obtain request failed.

A lock-obtain failure is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

000E Lock release request failed.

A lock-release failure is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

000F CVB is invalid.

The CVB control block represents the client connection. A CVB that is not valid is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

0010 Allocation of a message control block failed.

Message control blocks are used to move data traffic between VTAM and the client. If an allocation failure occurs, contact the IBM software support center.

0011 Work element Queue and Post request failed.

Internal Telnet work element processing failed. Contact the IBM software support center. PARM1 might contain an additional failure code to assist IBM software support to resolve the problem.

0012 Internal list request failed.

Internal list processing failed. Contact the IBM software support center.

0013 Available return code.

This return code is not used and is available for future use.

0014 CVB lock obtain request failed.

Lock processing of the CVB control block failed. This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

0015 CVB lock release request failed.

Lock processing of the CVB control block failed. This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

0016 CVB token is invalid.

The token for lock processing of the CVB control block is not valid. This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

0017 Available return code.

This return code is not used and is available for future use.

0018 Available return code.

This return code is not used and is available for future use.

0019 CVB token does not match master token.

The CVB token used by a particular process does not match the token stored in the Telnet tables. This event is sometimes part of normal processing when a session or connection is being dropped. If this event is reported at other times, contact the IBM software support center.

001A Telnet timer has been canceled.

The timers used for the INACTIVE and SCANINTERVAL options are canceled when the port is being stopped. If this event is reported at other times, contact the IBM software support center.

001B Takeover target is invalid.

Takeover was attempted on a target that cannot be taken over. A probable cause is that the profile used by the target did not specify takeover. Issue a detailed display of the original target connection. Check the profile flags to determine whether takeover is supported. If takeover is supported, contact the IBM software support center.

001C Copy of a message control block failed.

Message control blocks are used to move data traffic between VTAM and the client. If a copy failure occurs, contact the IBM software support center.

001D Duplication of a message control block failed.

Message control blocks are used to move data traffic between VTAM and the client. If a duplication failure occurs, contact the IBM software support center.

001E Internal Patricia tree process failed.

Internal Patricia tree processing failed during registration work. A possible cause is a takeover timing condition. Try the connection again. If the problem persists, contact the IBM software support center. PARM1 might contain an additional failure code to assist IBM software support to resolve the problem.

001F OE Dub Process failed.

Telnet initialization for socket setup failed with the BPX Dub process. Contact the IBM software support center. The PARM1 value is the z/OS UNIX System Services (USS) return value, the PARM2 value is the USS return code, and the PARM3 value is the USS reason code. They are defined in the z/OS UNIX System Services Messages and Codes.

0020 Dynamic LU tree creation failed.

The creation of the dynamic LU tree needed to track LU usage failed during Telnet initialization. Contact the IBM software support center.

0021 Patricia Tree ADD failed for IP node.

Internal Patricia Tree processing failed during profile IP node processing. An internal return code is saved in PARM1. If the problem persists, contact the IBM software support center.

0022 Patricia Tree DELETE failed for IP node.

Internal Patricia Tree processing failed during profile IP node processing. An internal return code is saved in PARM1. If the problem persists, contact the IBM software support center.

0023 Patricia Tree CREATE failed for IP node.

Internal Patricia Tree processing failed during profile IP node processing. An internal return code is saved in PARM1. If the problem persists, contact the IBM software support center.

0024 Patricia Tree token is invalid.

Internal Patricia Tree processing failed during profile IP node processing. An internal return code is saved in PARM1. If the problem persists, contact the IBM software support center.

0025 Takeover target is closing.

The target for connection or session takeover is in the process of closing. The takeover will not occur. The connection attempting the takeover should try the connection request again after receiving this message.

0026 Load of EZBTTMST load module failed.

Telnet Connection Manager load module could not be loaded. The most probable cause is that the load module is not part of the system library that is accessible to Telnet. The PARM1 value is the system completion code and the PARM2 value is the reason code. If the load module is accessible to Telnet, contact the IBM software support center.

0027 Load of EZBTPGUE load module failed.

Telnet User Exit Interface load module could not be loaded. The most probable cause is that the load module is not part of the system library that is accessible to Telnet. The PARM1 value is the system completion code and the PARM2 value is the reason code. If the load module is accessible to Telnet, contact the IBM software support center.

0028 Event should not occur. Call IBM service.

An event occurred in Telnet that should not have occurred. Contact the IBM software support center.

0029 Debug process called without setting up DUCB.

A TnDebug invocation occurred without first invoking the TnDebug entry with either the TASK or CONN option.

1001 Client disconnected from the connection.

The user or client emulator tried to end the connection by initiating a disconnection. If this return code is unexpected, analyze the client to determine why the client initiated a disconnection. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code. These values are defined in z/OS UNIX System Services Messages and Codes, or they might be set to an SSL/TLS error code. The SSL/TLS error codes are defined under return code 6002.

1002 Close socket request failed.

This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1003 A TCP/IP receive data request failed.

This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1004 A close request is already in progress.

A second close was attempted. The first close will continue and the second close will be ignored. If the first close does not complete, contact the IBM software support center.

1005 A Cancel socket I/O request failed.

This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1006 A TCP/IP send data request failed.

This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1007 Socket fastpath setup failed.

Telnet connection sockets are defined as fastpath to improve performance. If fastpath setup failure occurs, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1008 A Get Hostname by IP address request failed.

Telnet attempted to find the host name of the client but failed. The most probable cause is that the system DNS is not set up correctly. Ensure that the correct TCPIP.DATA statements are being used. Telnet uses the MVS™ search order. See z/OS Communications Server: IP Configuration Guide for information about the TCPIP.DATA file and search order. If this return code is unexpected, contact the IBM software support center. If the return code is part of a WLM failure message and Telnet is running in its own address space, the probable cause is that there is no affinity to a particular TCP/IP stack. Use the TCPIPJOBNAME parameter statement in the TELNETGLOBALS statement block to set affinity to a specific TCP/IP stack. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1009 Takeover has failed.

The new client has failed takeover, probably because the old client is still active. This return code is for tracking purposes and does not necessarily indicate a problem. The PARM3 value is the takeover type that was attempted.

100A Connection type of NONE was specified.

The profile option CONNTYPE NONE was specified indicating that no connections are allowed. If this result was not intended, reconfigure the Telnet profile.

100B Unexpected SSL handshake encountered.

An SSL handshake header was encountered on a basic port or the client immediately entered an SSL handshake for a CONNTYPE option value other than SECURE or ANY. Verify that the client and port settings are compatible.

100C A TCP/IP send immediate request failed.

This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

100D TCP/IP async send did not complete immediately.

A probable cause is a blocked socket. This condition should affect only the client that cannot accept additional data. If the entire server is affected, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

100E The transform task is not available.

The DBCS transform task is not available to perform the requested transformations. Either the DBCSTRANSFORM statement is missing, the load module did not get loaded, or the load module was removed because of an error. If an error occurred, contact the IBM software support center.

100F A send was issued without any data.

A request to send data to the client was issued but data was not specified. Contact the IBM software support center.

1010 The socket was dropped.

This event was probably caused by the operator. If not, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

1011 The transform request in PARM1 is invalid.

The transform request is not a valid request that can be handled by the transform process. Contact the IBM software support center. The request is reported in PARM1.

1012 A client doing a takeover is closing.

A new client began the close process while waiting for the takeover timer to expire. The new connection will finish closing after the takeover timer expires. If this return code is unexpected, contact the IBM software support center.

1013 Takeover already in progress.

A new client attempted to take over a connection that already is being taken over by another connection. Only one connection at a time can try to take over a connection.

1014 Takeover has started.

A new client began the takeover process. This return code is for tracking purposes and does not indicate a problem. The PARM1 value is the takeover time value specified on the particular takeover parameter in hexadecimal form. The PARM3 value is the type of takeover attempted.

1015 Takeover not specified on original client PROF.

A new client attempted to take over a connection but the original connection does not allow takeover. Takeover must be specified on the profile used by the original connection. The new client might not be attempting takeover and instead accidentally chose an LU already in use. In this case, the client should use a different LU name.

1016 Port Task setup failed.

The setup of the port task failed. The port will not be available. The task was set up and the Port task code began to run, but an error occurred during initialization. The PARM1 value is the port task return code. the PARM2 value is the hexadecimal value of the port number. Contact the IBM software support center.

1017 Attach of the Port task failed.

The MVS macro, ATTACH, failed to attach the port task during Telnet initialization. The PARM1 value is the ATTACH return code. The PARM2 value is the hexadecimal value of the port number. Contact the IBM software support center.

1018 The Port task has ended in error.

The port task ended because of one of the following error conditions.

- Instance 01 indicates that the task was set up correctly and that later an error occurred. The PARM1 value is the port task return code.
- Instance 02 indicates that the task was set up, but the port task code never ran. The PARM1 value is a system completion code.
- Instance 03 indicates that the task was set up, the port task code was initialized, but an error quickly occurred. The PARM1 value is the port task return code.

In all cases, the PARM2 value is the hexadecimal value of the port number. Contact the IBM software support center.

1019 The connection ID could not be obtained.

The request by Telnet to get the connection ID for this connection failed. The connection request will fail. Contact the IBM software support center. The PARM1 value is the return value, the

PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

101A Setup of Out Of Band data handling failed.

The request by Telnet to handle out-of-band data inline failed. The connection request will fail. Contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code; these values are defined in z/OS UNIX System Services Messages and Codes.

101B The linkname table could not be obtained.

The request by Telnet to get the TCP/IP stack link name table failed. The connection will continue but any profile mappings based on the link name will fail. Contact the IBM software support center.

101C Send data to the client.

The Debug Trace option was selected, resulting in trace messages for two connections. The PARM1 value is the total length sent.

101D Receive data from the client.

The Debug Trace option was selected, resulting in trace messages for two connections. The PARM1 value is the total length received.

101E The profile control block could not be found.

The most probable cause is that all the port profiles are qualified and the connection request has a different destination IP address or link name than any that are defined. If only the qualified port destinations are to be used, then this is probably not an error. In that situation you can create a non-qualified profile to cover unexpected connections.

101F There are no current profiles available.

There are no profiles available for the connection to use. Contact the IBM software support Center.

1020 The main connection CB could not be obtained.

The control block structure that manages connections could not be obtained. The most probable cause is that storage is not available. Verify that storage is available. If a storage shortage is not the problem, contact the IBM software support center.

1021 The takeover connection is now invalid.

While the connection that is being taken over is closing, the takeover connection became unusable. The most probable cause is that the connection is being disconnected by the user. The PARM1 value is an additional failure code to assist IBM software support to resolve the problem.

1022 VTAM Appl sent Bind before negotiation complete.

TKO takeover is in process and the VTAM application tried to start a session before the TKO Taker negotiations were complete. This event can cause many timing problems. The takeover will end and the client will be disconnected.

1023 Telnet does not support the exit type.

The Telnet common exit processor was given control to process an exit type other than an interpret exit or LU name exit. This event should not occur. Contact the IBM software support center. The PARM1 value is the exit type code that was attempted.

1024 Adding Userid information for keep LU failed.

While the LU is being unassigned, the client identifier user ID information could not be saved. The most probable cause is a storage shortage. If a storage shortage is not a problem, contact the IBM software support center.

1025 Adding hostname information for keep LU failed.

While the LU is being unassigned, the client identifier host name information could not be saved. The most probable cause is a storage shortage. If a storage shortage is not a problem, contact the IBM software support center.

1026 Adding IP addr information for keep LU failed.

While the LU is being unassigned, the client identifier IP address information could not be saved. The most probable cause is a storage shortage. If a storage shortage is not a problem, contact the IBM software support center.

1027 Last send not ACKed. Stack drops connection.

The request by Telnet to send to the client did not get an acknowledgement in the maximum retry limit. The connection is reset by the stack.

1028 Failed to get SecLabel for Incoming connection.

The request by Telnet to get the security label value of the incoming connection failed. The security label option is required for TN3270 because multilevel security has been activated in the security server.

1029 The zonename table could not be obtained.

The request by Telnet to get the TCP/IP stack zone name table failed. The connection will continue but the zone ID of this connection will not be known. Contact the IBM software support center.

102A Takeover attempted with a different IP address.

A new client attempted a session reconnect takeover using a different IP address than the original connection. SAMEIPADDR was specified for takeover on the original connection.

102B Socket initialization failed. No retry.

The socket initialization failed and will not be tried again. Message EZZ6011I should have been issued before the debug message with this code. Message EZZ6011I should describe why the socket did not initialize.

102C Socket initialization failed. Will retry.

The socket initialization failed but will be tried again in 10 seconds and then tried again indefinitely with progressively longer wait periods. The most probable reason for retry is that Telnet is running in its own address space tried to open a socket to a TCP/IP stack that is not active.

102D TCPIP environment changed. Port cannot start.

Telnet detected an IPv4 or IPv6 environment change or a CINET or INET environment change since the last port was opened. Stop and restart the Telnet server when an environment change is made.

102E Telnet could not get TCPIP stack information.

Telnet running in its own address space could not retrieve the identity of the TCP/IP stack for the connection that was just established. The connection will complete but displays that are dependent on the owning stack of the connection will not function.

1030 TTLS Ioctl failed for query or init HS.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code for the ioctl failure; these values are defined in z/OS UNIX System Services Messages and Codes.

1031 BPX1FCT failed changing socket blocking status.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code for the ioctl failure.

1032 The connection state is invalid for CONNTYPE.

The PARM2 value is the CONNTYPE statement value and the PARM3 value is the connection status.

1033 Cleartext received when CONNTYPE is secure.

Cleartext data is either already on the TCPIP receive queue when the handshake starts or it arrives while waiting for the handshake to start. The CONNTYPE statement does not allow negotiation to a basic connection.

1034 The Poll for write to detect HS complete failed.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code for the ioctl failure.

1035 Policy is invalid for the CONNTYPE specified.

The PARM2 value is the CONNTYPE statement value and the PARM3 value is the policy status.

1036 Takeover target uses different connection type.

A new client attempted a session reconnect takeover of a connection of a different connection type. The takeover attempt fails. This error might occur when SAMECONNTYPE is specified for the original connection and one of the following is true:

- A secure connection attempted to take over a basic connection.
- A secure connection that was using client authentication attempted to take over a secure connection that did not use client authentication.

2001 ACB mismatch during Bind processing.

The ACB address in the bind does not match the ACB representing the connection. If the application does not appear to be at fault, contact the IBM software support center. A VTAM internal trace in addition to the Telnet debug information will be needed.

2002 Available return code.

This return code is not used and is available for future use.

2003 Available return code.

This return code is not used and is available for future use.

2004 Available return code.

This return code is not used and is available for future use.

2005 The session is not a SNA session.

Session verification indicates this is not a SNA session but this session is attempting to perform a SNA-type function. If you require SNA function, change the Devicetype logmode.

2006 Error writing SMF record.

An error occurred while attempting to write an SMF record. Contact the IBM software support center. PARM1 might contain the SMF return code to assist IBM software support to resolve the problem.

2007 VTAM macro RECEIVE failed.

This event is sometimes part of normal processing when a session or connection is being ended. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2008 A response to VTAM failed.

An error occurred while attempting to send a response to VTAM. This event is sometimes part of normal processing when a session or connection is being ended. If this event is reported at other times, contact the IBM software support center.

2009 Sending UNBIND to client failed.

A probable cause is a BIND was not already sent to the client. Verify that the application is sending the correct sequence of BINDs and UNBINDs. If the application does not appear to be at fault, contact the IBM software support center. The PARM1 value is an additional return code indicating why the SEND failed.

200A NSEXIT was driven for a BIND failure.

The Telnet LU network services exit was driven, which indicates that a BIND request failed. Review VTAM messages for possible causes.

200B Sending BIND to client failed.

A probable cause is a BIND that was already sent to the client. Verify that the application is sending the correct sequence of BINDs and UNBINDs. If the application does not appear to be at fault, contact the IBM software support center. The PARM1 value is an additional return code indicating why the SEND failed.

200C RPLRQR,RPLSTSN not valid for TS profile 2/3.

The RPLRQR and RPLSTSN profiles are not valid for TS profiles 2 or 3. Because these are the only profiles that the Telnet server supports, this error should not occur. If this error does occur, analyze why the host application is sending these requests and change the application.

200D Received BIND while already bound.

Verify that the application is sending the correct sequence of BINDs and UNBINDs. If the application does not appear to be at fault, contact the IBM software support center.

200E Invalid TERMSESS type encountered.

The VTAM macro TERMSESS was requested with an internal function code that was not valid. Contact the IBM software support center.

200F VTAM macro TERMSESS failed.

This event is sometimes part of normal processing when a session or connection is being ended. If this event is reported at other times, contact the IBM software support center. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2010 VTAM macro OPNSEC failed.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2011 VTAM macro REQSESS failed.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2012 VTAM macro CLOSE ACB failed.

PARM1 and PARM2 might be set to return code and reason code respectively, which are defined in z/OS Communications Server: SNA Programming.

2013 VTAM macro OPEN ACB failed.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the ACB error flag value; these values are defined in z/OS Communications Server: SNA Programming. The most probable cause is that the LU is not active in VTAM. Issue D NET,ID=luname to see the VTAM status of the LU.

2014 VTAM macro SETLOGON failed.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2015 NSEXIT was driven for session cleanup.

A probable cause is that the host application was deactivated. Review VTAM messages for other possible causes.

2016 NSEXIT was driven for a CINIT failure.

The Telnet LU network services exit was driven, which indicates that a CINIT request failed. Review VTAM messages for possible causes.

2017 NSEXIT was driven for a CTERM failure.

The Telnet LU network services exit was driven, which indicates that a CTERM request failed. Review VTAM messages for possible causes.

2018 NSEXIT was driven for an UNBIND failure.

The Telnet LU network services exit was driven, which indicates that an UNBIND request failed. Review VTAM messages for possible causes.

2019 Session does not exist.

Session verification determined that a session no longer exists. The attempted function is not performed. This event is sometimes part of normal processing when a session is ended. If this event is reported at other times, contact the IBM software support center.

201A Session data queue is being purged.

The host application sent a CLEAR option to purge the data queue. New data cannot be added until the CLEAR option is complete.

201B Available return code.

This return code is not used and is available for future use.

201C Available return code.

This return code is not used and is available for future use.

201D Available return code.

This return code is not used and is available for future use.

201E Available return code.

This return code is not used and is available for future use.

201F Available return code.

This return code is not used and is available for future use.

2020 VTAM RECEIVE macro requested invalid function.

Request parameter list (RPL) verification determined that an unrecognized function was attempted during the VTAM RECEIVE process. Verify that the application is sending valid RPL requests. If the application does not appear to be at fault, contact the IBM software support center. A VTAM internal trace in addition to the Telnet debug information will be needed.

2021 Available return code.

This return code is not used and is available for future use.

2022 Already pending response. SNA protocol error.

This return code is caused by an APPL sending in a definite response required RU and a response is already pending from the client. The session is terminated.

2023 Retry scheduled for RPL request.

A probable cause for the failure is a temporary storage shortage in VTAM. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2024 RPL length specified but RPL area is zero.

Request parameter list (RPL) verification determined that the RPL length field is set but the RPL area field is 0. Storage corruption is the probable reason. Contact the IBM software support center.

2025 Available return code.

This return code is not used and is available for future use.

2026 Available return code.

This return code is not used and is available for future use.

2027 Maximum retries exceeded for VTAM RPL.

A probable cause for the failure is a temporary storage shortage in VTAM. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2028 Available return code.

This return code is not used and is available for future use.

2029 VTAM RPL posted with nonzero RPLrtncd/RPLfdbk2.

A minor error was reported in a VTAM RPL request. The session will not be ended. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

202A VTAM RPL returned negative response.

A negative response was returned from a VTAM RPL macro. The session will be ended. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

202B Available return code.

This return code is not used and is available for future use.

202C Available return code.

This return code is not used and is available for future use.

202D VTAM macro SEND expedited failed.

SHUTC and SIGNAL are expedited RPLs. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

202E VTAM macro REQSESS failed. Already in session.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

202F BIND for printer received with invalid LU.

The BIND received from the host application did not specify an LU1 or an LU3. Determine why the application sent a BIND that was not valid.

2030 Sending a response to VTAM when none expected.

The client sent a response to Telnet that should be passed through to VTAM. In this case, Telnet does not expect that the application should be sent a response. This event is sometimes part of normal processing when a connection is being dropped. If this event is reported at other times, contact the IBM software support center.

2031 Abnormal termination of request.

VTAM abnormally terminated a request because an error was detected while the request was being processed or because a session, task, or address space error occurred. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd or / RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2032 Receive negative response and continue process.

A negative response was received from the host application with a sense code that indicates that the session should not be ended.

2033 Send data attempted without having SDT.

A send data request is rejected because a start data traffic (SDT) request was not received. Either the initial SDT was not received or a CLEAR was received and a new SDT was not received.

2034 Specified maximum ReqSess attempts exceeded.

The connection appears to be in a CLSDST PASS loop. The number of request session attempts in a 10-second period exceeded the number specified on the MAXREQSESS statement or the default. The PARM1 value is the limit value in hexadecimal format. The count is incremented when a BIND is received from the host application.

2035 UNBIND or CLEAR ended a RECEIVE request.

The VTAM application issued an UNBIND or CLEAR request that ended the RECEIVE RPL request. The connection is kept, waiting for the follow-up process from the application. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the RPLrtncd and RPLfdbk2; these values are defined in z/OS Communications Server: SNA Programming.

2036 Send data to the VTAM application.

The Debug trace option was selected, causing trace messages for two connections. The PARM1 value is the total length sent.

2037 Receive data from the VTAM application.

The Debug trace option was selected, causing trace messages for two connections. The PARM1 value is the total length sent.

2038 BIND specifying delayed response mode received.

The BIND received from the host application specifies delayed response mode. Although this BIND will be accepted, the Telnet server does not support delayed response mode. Multiple outstanding requests for definite responses from the host application can cause sessions to be stalled. Determine why the application sent the BIND with delayed response mode specified.

2039 Receive BIND from the VTAM application.

The Debug trace option was selected, which caused trace messages for two connections. The PARM1 value is the total length sent. The PARM2 value is the Request/Response header (RH) fields.

2040 Receive UNBIND from the VTAM application.

The Debug trace option was selected, which caused trace messages for two connections. The PARM1 value is the total length sent. The PARM2 value is the RH fields.

2041 Issue TERMSESS to the VTAM application.

The Debug trace option was selected, which caused trace messages for two connections. The PARM1 value is the total length sent. The PARM2 value is the RH fields.

2042 LU Group Invalid in MLS Environment.

The LU group has been flagged as being not valid in the current multilevel security environment. Either an LU exit does not have an LU or the first LU defined for the LU group does not have a security label value defined in the security server.

2043 Issue SETLOGON to the VTAM application.

The Debug trace option was selected, which caused trace messages for two connections. The PARM1 value is the total length sent. The PARM2 value is the RH fields.

2044 OPEN ACB failed twice for a TN3270E LUNAME.

A TN3270E connection receives the LU name allocated as soon as the device type is known. If this LU name is not active in VTAM when the OPEN ACB macro is processed, the OPEN fails. The LU name is deactivated now, but the LU name remains associated with the connection because the client knows the LU name. If the client enters a new application, OPEN ACB will fail again. When this occurs, the connection will be dropped with the 2044 error code to prevent a loop with a screen scraper program running.

2045 VTAM SCIP exit rejects APPL data. Conn Closing.

An application sent data to the SCIP exit of the Telnet LU representing the connection. The connection is closing and the data is rejected. The connection might be closing only the session, but the data was sent before the Telnet LU was ready to receive more data. If this timing condition exists, review the function of the application as a partner with a Telnet LU.

3001 The LU is in use and cannot be inactivated.

The LU name being deactivated is in use by a Telnet connection. The LU name cannot be deactivated while it is in use.

3002 The LU was inactive before the request was made.

The LU name specified was already inactive before the INACT or assignment request was made. The LU name must be activated before it can be used.

3003 LUs are all in use.

The specific LU requested is in use or a generic request mapped to an LUGROUP or DEFAULTLUS pool that has no LUs available. Verify that the profile mapping statements are correct and that sufficient LUs are available. TN3270E connections are assigned LUs whether or not a session is established. Be sure to account for this additional LU usage by adding additional LUs, if necessary. The PARM3 value might be the LU group name or the exact LU name for which the assignment failed. If multiple LU groups or exact LU names are mapped to the client identifier, only the last name will be displayed, which indicates that assignment failed for all mappings. If the reporting module is EZBTXUTL, the PARM2 value is the LU group name and the PARM3 value is the LUNR system and job name.

3004 LU is not available.

There is not an LU mapping for this client or, the connection requests a specific LU, there is not an LU definition that matches the LU name on the request. Verify that the profile mapping statements are correct.

3005 Database error - Invalid database header.

A database header that was not valid was detected. A probable cause is storage corruption. Contact the IBM software support center.

3006 Specific requests are only valid in TN3270E.

A specific LU connection request was attempted on a non-TN3270E connection. Verify that NOTN3270E is not coded and check the client to confirm a TN3270E connection was requested. Some clients allow a specific LU request on a TN3270 connection that is not supported on this server.

3007 Invalid map index has been detected.

LU map index verification detected an error. Contact the IBM software support center.

3008 Invalid application index has been detected.

Application LU map index verification detected an error. Contact the IBM software support center.

3009 Available return code.

This return code is not used and is available for future use.

300A Invalid bundle index has been detected.

An internal index that was not valid was detected. Contact the IBM software support center.

300B Telnet LU not in use.

Telnet attempted to make an LU that is not registered as being in use available during close processing. Contact the IBM software support center.

300C Database headers in the TCFG are corrupted.

One or more database headers in the profile control block, TCFG, are corrupted. Contact the IBM software support center.

300D The LU is not associated with this connection.

The close process is attempting to make an LU available that Telnet expects to be associated with the connection. In fact, no LU was associated with the connection. Contact the IBM software support center.

300E Invalid indices have been detected in the TCFG.

The profile control block, TCFG, has one or more indices that are not valid. A probable cause is storage corruption. Contact the IBM software support center.

300F Linkname Lookup failed.

During profile processing, a client identifier was checked to determine whether it was a link name. In this case, the name on the profile mapping statement is not a link name.

3010 Lookup request is invalid.

An internal lookup request is not valid. Contact the IBM software support center.

3011 Application name is required.

An application name is required for a session to be established. This return code is part of normal processing whenever a USSMSG10 or solicitor panel is sent to the client. This error can also occur when the user did not enter an application name when prompted to do so.

3012 Application name is invalid.

The application name entered by the user is not valid, based on the ALLOWAPPL or RESTRICTAPPL statements in the profile. Be sure that the user is requesting a valid name. Also, be sure that any applications that are the target of a CLSDST PASS macro are in the profile table. For example, a logon to TSO causes a CLSDST PASS to TSO0001. An ALLOWAPPL TSO* statement is required for the second TSO application name to be valid.

3013 Application name has a syntax error.

The application name entered by the user contains a syntax error. Application names must be 1-8 characters in length. The first character must be one of the following: A-Z @ # $. The second through eighth character must be one of the following:A-Z 0-9 @ # $.

3014 Userid is required.

The application name requested by the user is a RESTRICTAPPL statement. The USERID specified is not listed on the RESTRICTAPPL statement.

3015 Userid and password are required.

The application name requested by the user is a RESTRICTAPPL statement that requires the entry of a user ID and password before the session can be established.

3016 Password is required.

The application name requested by the user is a RESTRICTAPPL statement that requires the entry of a password before the session can be established.

3017 Password is invalid.

The password entered by the user is not valid. Reenter the correct password or contact your local system or security administrator.

3018 Password is expired.

The password entered by the user has expired. The user needs to enter a new password.

3019 Password is revoked.

The password entered by the user was revoked. Contact your local system or security administrator.

301A Password not in the security program.

The password entered by the user could not be found in the security system. Contact your local system or security administrator.

301B Password failed in the security program.

The password entered by the user failed in the security system for an unknown reason. Contact your local system or security administrator.

301C Password failed in the security system group.

The password entered by the user was not part of the security system group. Contact your local system or security administrator.

301D System security password group revoked.

The user ID entered by the user is part of a group that was revoked. Contact your local system or security administrator.

301E Password change requires old and new password.

When changing a password, both the old and new passwords must be entered.

301F New password is invalid.

When changing a password, the new password must meet certain password formatting rules. Contact your local system or security administrator for details.

3020 New password change failed.

An unknown failure occurred while trying to change the password. Contact your local system or security administrator.

3021 Associated printer already in use.

The associated printer is already in use by another Telnet connection. Try specifying another printer name or wait until the other connection is dropped.

3022 Associated terminal is invalid.

The terminal LU specified on the associated printer connect request is not valid. The terminal LU name used for the association is not a valid terminal LU name. Using a client trace or DEBUG TRACE, verify that the correct terminal LU name is on the associated connect request. If it is, contact the IBM software support center.

3023 Associated printer list size is incorrect.

The printer LU group and the terminal LU group must be the same size. The number of single entries must match, the number of bundle entries must match, and the number in each bundle must match. Verify that the LUGROUP and associated PRTGROUP pools do have the required one-to-one match-ups required.

3024 Available return code.

This return code is not used and is available for future use.

3025 System security request is invalid.

Telnet issued a system security request that was not valid. Contact the IBM software support center.

3026 System security STAT request failed.

CLIENTAUTH SAFCERT statement requested but the security product is not active. Ensure that the security product is active before using CLIENTAUTH SAFCERT. The PARM1 value is the return code, the PARM2 value is the SAF return code, and the PARM3 value is the SAF reason code from the RACROUTE FASTAUTH request.

3027 Client not authorized to use the port.

CLIENTAUTH SAFCERT was specified for the connection. The user ID associated with the client certificate does not have read access to the port resource and the connection is closed.

The PARM1 value is the return code, the PARM2 value is the SAF return code, and the PARM3 value is the SAF reason code from the RACROUTE FASTAUTH request. Contact your local system or security administrator if this client requires access.

3028 System security client certification failed.

CLIENTAUTH SAFCERT was specified for the connection and the client certificate is not registered with the security product. Contact your local system or security administrator if this client requires access. The PARM1 value is the SAF return code.

3029 INITACEE is not available.

CLIENTAUTH SAFCERT was specified for the connection. However, the security product does not support client certificate queries. Contact your local system or security administrator.

302A Associated connect request is invalid.

The associated connect request is invalid. The requester might not be a printer or the associated LU name is blank.

302B Associated terminal LU is not assigned.

The terminal LU must be assigned before the printer can issue an associated connect request. The LU is not assigned.

302C No printer group associated with Terminal LU.

An associated connect request was received that contained a terminal LU name that does not have an associated printer. A probable cause is that the terminal LU was mapped to an LU group on an LUMAP statement that does not have an associated printer pool defined. Verify that the client is using an LU from an LUMAP statement that has an associated printer pool defined.

302D LU lookup confirmation failed.

Lookup is often performed more than once. For example, a TN3270E connection is assigned an LU during connection negotiation. Later, another lookup is performed that includes the application name. These later lookups confirm that the LU assigned earlier is still correct. In this case, confirmation failed. Contact the IBM software support center.

302E TakeoverRecon with a different APPL attempted.

An end user is attempting a session reconnect takeover and is specifying a different application name than the original session used. The original session is dropped and takeover is performed without the reconnect function.

302F System security user profile not defined.

The user profile is not defined in the system security application. Contact your local system or security administrator.

3030 TakeoverRecon with a different USERID attempted.

An end user is attempting a session reconnect takeover and is specifying a different user ID than the original session used. The original session is dropped and takeover is performed without the reconnect function.

3031 Specified different applname when DEFONLY coded.

The default application name on the DEFAULTAPPL, PRTDEFAULTAPPL, LINEMODEAPPL, or LUMAP-DEFAPPL statement has DEFONLY coded. This means that the user can log on only to that application. In this case, the user attempted to log on to a different application name from a USS screen or the solicitor panel. These screens can be sent because of a logon error, logoff of a logappl session, or logoff of a session when FIRSTONLY is coded.

3032 Invalid Client Identifier type.

An internal error caused an invalid client identifier to be used. The PARM1 value is the hexadecimal value of the client identifier. Contact the IBM software support center.

3033 Invalid Object type.

An internal error caused an invalid object to be used. The PARM1 value is the hexadecimal value of the client identifier. Contact the IBM software support center.

3034 The Object group has no entries.

An object group has no valid object entries. The PARM3 value is the group name. Determine the errors in the group and try the profile again.

3035 The Client Identifier has no entries.

A client identifier has no valid client identifier entries. If the client identifier is a group, the PARM3 value is the group name. Any mapping statement using this client identifier will fail. Correct the client identifier errors in the group or on the mapping statement and try the profile again.

3036 Invalid parms were encountered.

Invalid parameters were encountered while processing the statement. Review the syntax for the statement in the z/OS Communications Server: IP Configuration Reference.

3037 Invalid mapping statement.

An internal error caused an invalid mapping statement to be used. The PARM1 value is the hexadecimal value of the mapping statement. Contact the IBM software support center.

3038 Mapping of the Client Identifier failed.

A valid client identifier could not be found for this mapping statement. The most probable cause is using a Group name before the group is identified.

3039 Mapping of the Object failed.

A valid object could not be found for this mapping statement. The most probable cause a group name was used before the group was identified.

303A The mapping statement is a duplicate.

The mapping statement is an exact duplicate of an earlier mapping statement. The PARM3 value is the last 22 characters of the data set name. If the data set name is longer than 22 characters, the PARM3 value starts with two dots (..) followed by the last 20 characters of the data set name.

303B Object mapped to Client Identifier is replaced.

The DEFAULTAPPL, PRTDEFAULTAPPL, LINEMODEAPPL, USSTCP, and INTERPTCP options allow only one object to be mapped to a client identifier. An earlier statement mapped a different object to the client identifier on the current line. The PARM1 value is the old object name and the PARM3 value is the new object name.

303C A hash entry was not found.

No host name, link name, or user ID hash table entry was found during delete processing. If the problem continues, contact the IBM software support center.

303D Available return code.

This return code is not used and is available for future use.

303E Invalid LU name from LU exit, client, or profile.

The connection request being processed is ended because the name is not valid. If the LU name was assigned by an LU exit, correct the exit to avoid the naming error. If the LU name was requested by the client, either the name specified at the client is incorrect or a group name was specified and the group name does not exist in the profile. Check the name specified at the client. If the name is correct, verify that the LU group name exists in the current profile. If the LU name was on a mapping statement, either the name was specified incorrectly or the name is a group name but the group was not created before the mapping statement was processed.

303F Invalid LUGROUP name.

The LU group name specified on the ALLOWAPPL or RESTRICTAPPL statement is not valid. The probable cause is that the LU group was not defined earlier. The PARM3 value is the LU Group name that is not valid.

3040 Multiple LUGROUPs were specified. Last one used.

Multiple LU groups were defined on the ALLOWAPPL or RESTRICTAPPL statement. The last LU group specified is used and is contained in the PARM3 value.

3041 LUG parameter is used instead of single LUs.

One or more LU groups were defined along with single LUs on the ALLOWAPPL or RESTRICTAPPL statement. The last LU group specified is used and is contained in the PARM3 value.

3042 The LU being activated is not on inactive list.

The LU name being activated is not on the inactive list and therefore cannot be activated. Use the INACTLUS display command to determine which LU names are inactive.

3043 No LU in mapped groups for KEEPLU or TKOGENLU.

Either the KEEPLU function or the Generic Takeover function is using a suggested LU that does not match any LU in the mapped LU groups for this connection. The saved LU name for the original connection might have been saved based on the SSL user ID or host name and the LU group

mappings might be based on the IP address. This can cause a mismatch. The PARM1 value is the LU name that did not match in any LU group mapped to the connection.

3044 User id longer than express logon symbolic.

The user ID that was returned by security lookup for express logon is longer than the symbolic user ID field. A seven character symbolic user ID was being used but an eight character user ID was returned. The length of the user ID that is returned must be equal to or shorter than the length of the symbolic user ID. Either use the eight character symbolic user ID or use seven character or shorter user IDs.

3045 Duplicate RESTRICTAPPL userid. Last one is used.

The same user ID was specified more than once on the RESTRICTAPPL statement. The PARM3 value is the duplicated user ID.

3046 Available return code.

This return code is not used and is available for future use.

3047 Available return code.

This return code is not used and is available for future use.

3048 Allowappl name invalid. Already a Restrictappl.

The application name contained in the PARM3 value was already defined as a RESTRICTAPPL statement and cannot now be defined as an ALLOWAPPL. Be sure that the application name is correct on each statement.

3049 Invalid Object Function.

An invalid object function, contained in PARM1, was requested during database processing. Contact the IBM software support center.

304A Invalid Client ID Function.

An invalid client ID function, contained in PARM1, was requested during database processing. Contact the IBM software support center.

304B Same name Allowappl is being replaced.

An earlier ALLOWAPPL statement with the same application name that is in the PARM3 value is being replaced by the current statement. Be sure that each statement has the correct application name specified.

304C Same name Restrictappl is being replaced.

An earlier RESTRICTAPPL statement with the same application name that is in the PARM3 value is being replaced by the current statement. Be sure that each statement has the correct application name specified.

304D LU range lower base does not match upper base.

The LU range shown in the PARM3 value does not have the same base portion in the lower and upper range names.

304E LU range lower base is higher than upper base.

The lower base LU name in the LU range shown in the PARM3 value has a higher value than the upper base LU name in the range. Correct the range so that the lower base LU name has a lower value than the upper base LU name.

304F LU range variant larger than 4B. Range ignored.

The LU range shown in the PARM3 value will generate a range larger than 4294967296 (4B), which is invalid. Reduce the range to be less than 4294967296 (4B).

3050 LU range started as numeric. cannot have alpha.

The LU range shown in the PARM3 value is assumed to be numeric but an alphabetic character was found in the variant portion. Change the range so that it contains only numeric characters.

3051 LU range started as alpha. cannot have numeric.

The LU range shown in the PARM3 value is assumed to be alphabetic but a numeric character was found in the variant portion. Change the range so that it contains only alphabetic characters.

3052 This LUMAP replaces earlier LUMAP with same LU.

The LU or group name contained in the PARM3 value is used in an earlier LUMAP statement with different parameters. The current statement replaces the earlier statement. Be sure that each statement is coded correctly.

3053 Client ID already used, cannot be used again.

The client identifier contained in PARM1 was used earlier. If the identifier was used in a group, the PARM3 value is the previous group name. The original identifier is used and this entry is ignored. Be sure that each was coded correctly. When the Client ID is an IP address, PARM1 will contain the hexadecimal value of the last 4 bytes only.

3054 An internal error caused Inactivation failure.

An internal error did not allow the LU inactivation to complete. The most probable causes are storage shortage or corruption of a data structure. Contact the IBM software support center.

3055 Available return code.

This return code is not used and is available for future use.

3056 The LuMap LuGroup does not contain assigned LU.

The LU group assigned to the connection now does not contain the LU name that was already assigned to the connection. This event is probably caused by having multiple LUMAP statements for the same client identifier, which can change based on the application name chosen.

3057 The Appl LuGroup does not contain assigned LU.

The LUs assigned to the chosen application do not match the LU name that was already assigned to the connection. This event is probably caused by having LUs listed in the LU group on the LUMAP statement that are not listed in the LU group (or LU list) assigned to the application.

3058 An invalid range was specified.

The range specified during storage cleanup was not found. The most probable cause is storage corruption. Contact the IBM software support center.

3059 No ParmsGroup defined for PMAP on LU/PRTMAP.

An LUMAP or PRTMAP statement specified an associated ParmsGroup statement using the PMAP parameter. The associated ParmsGroup name could not be found. The associated ParmsGroup statement must be defined before the mapping statement.

305A The password was successfully changed.

The Telnet solicitor panel was used to change an existing password. The change was successful.

305B The requested LU is kept for another client.

The LU name requested cannot be used now because it is being kept for another client that has previously used the LU name. When the KEEPLU statement time expires, the LU will be available to other clients.

305C Earlier ParmsGroup map replaced with this one.

The same ParmsGroup statement was mapped to the same client identifier more than once. The last mapping is used to concatenate the parameter values.

305D Assoc printer/terminal LU profile mismatch.

The printer connection must be assigned the same profile as the terminal LU. The printer connection will be rejected if a VARY TCPIP,,OBEYFILE command update is performed between the terminal LU connections and the printer connection or if the printer connects to a port different from the terminal LU port.

305E No common LU name in both LUMAP & APPL LU sets.

The LU group or single LU defined to the connection by the LUMAP statement or default LU group does not contain an LU name that matches any LU associated with the application by the ALLOWAPPL or RESTRICTAPPL-USER statement.

305F The LU is already locked. Pass to next LU.

The LU that was selected is already locked by another process. The generic search immediately passes to the next LU.

3060 WLMCLUSTERNAME must have stack affinity.

The WLMCLUSTERNAME parameter statement has been coded. When this parameter is specified, the TCPIPJOBNAME parameter statement must also be coded to ensure stack affinity.

3061 Profile is being cleaned up but has connections.

A profile is being cleaned up when the port is ending. A connection count check was performed to ensure that all connections were cleaned up, but the check found that not all connections were cleaned up. Contact the IBM software support center.

3062 LU is inactive on LUNR.

A shared LU was assigned to a connection on the LUNR. The LU was already marked as inactive on the LUNR. The LU will be marked as inactive on the LUNS. The LU must be activated on the LUNR and the LUNS before it can be assigned again.

3063 LU is active on LUNR.

A shared LU was assigned to a connection on the LUNR. The LU was already marked as active on the LUNR. The LU will be marked as inactive on the LUNS. Ensure that the LU is not defined in any nonshared groups on the LUNR. The LU must be activated on the LUNS before it can be assigned again.

3064 LU is not known to VTAM on LUNR.

A shared LU was assigned to a connection on the LUNR. The LU was not known to VTAM and the session could not be opened using this LU. The LU will be marked as inactive on the LUNS. The LU must be defined to VTAM on the LUNR and activated on the LUNS before it can be assigned again.

3065 LU is already active to VTAM on LUNR.

A shared LU was assigned to a connection on the LUNR. The LU was already active to VTAM and the session could not be opened using this LU. The LU will be marked as inactive on the LUNS. Ensure that the LU is not locally defined to any other LUNR. The LU must be activated on the LUNS before it can be assigned again.

3066 Incorrect use of VREQ continuation.

An internal error occurred while processing a configuration statement. Contact the IBM software support center.

4001 Available return code.

This return code is not used and is available for future use.

4002 TN3270E header is in error.

The TN3270E header in the message received from the client contains an error. Using a client trace, analyze the header. If the header seems to be correct, contact the IBM software support center.

4003 SSCP LU data is invalid.

Telnet received 3270 data, a response, or is still in session when the connection is in SSCP-LU mode. Use a client trace or a DEBUG CONN TRACE statement to verify that the client does not send 3270 data or a response after issuing a SYSREQ statement to change to SSCP-LU mode.

4004 TN3270E subfunction was not negotiated.

The function requested by the client in the TN3270E header was not negotiated to be supported during connection startup. Use a client trace or DEBUG TRACE statement to identify the unsupported function and determine why the client is requesting a function that is not supported.

4005 TN3270E datatype is not supported.

Telnet does not accept BIND, UNBIND, or NVT data from the client. Determine why the client is sending this data.

4006 Data received from the client is invalid.

Probable causes include receiving a TN3270E header with no data or receiving a response with an invalid flag value. See RFC 2355 for valid response values. Using a client trace or DEBUG TRACE, determine which data is not valid and why the client is sending this data. See Related protocol specifications for information about accessing RFCs.

4007 VTAM Rsp received but previous rsp not complete.

A response was received from VTAM before an earlier response was completed. Contact the IBM software support center.

4008 VTAM Rsp received but was not expected.

A response was received from VTAM but Telnet was not expecting a response. Contact the IBM software support center and provide a VTAM internal trace and the Telnet debug information.

4009 Negative VTAM Rsp is invalid.

A negative response from VTAM was received with sense information that is not valid, according to RFC 2355. Determine why the application sent the invalid sense information and change the application. See Related protocol specifications for information about accessing RFCs.

400A Printer data is invalid.

Telnet received either SCS data or 3270 data. These datatype are not supported by the client, according to connection negotiation. Check the client to determine whether the data type option can be turned on or off. Otherwise, use a client trace or DEBUG TRACE during connection setup to verify what options are supported.

400B No data to send to the client.

A request parameter list (RPL) was received from VTAM. Telnet determined that no data is available to send to the client. Contact the IBM software support center.

400C BIND being sent to the client is invalid.

Probable causes are a BIND was already sent to the client or the BIND is zero length. Verify that the application is sending the correct sequence of BINDs and UNBINDs. If the application does not appear to be at fault, contact the IBM software support center.

400D UNBIND being sent to the client is invalid.

Probable causes are an UNBIND was already sent to the client, a BIND was never sent, or the UNBIND is zero length. Verify that the application is sending the correct sequence of BINDs and UNBINDs. If the application does not appear to be at fault, contact the IBM software support center.

400E Attempt to send BIND to client in SSCP-LU mode.

A request to send a BIND to the client is refused because the connection is in SSCP-LU mode. The client cannot accept binds.

400F Amount of data exceeded MAXRECEIVE value.

The amount of data received without an end-of-record indicator exceeded the value coded on the MAXRECEIVE statement or it exceeded the default value. A probable cause is a broken client is in a send loop or a corrupted data length that is large was used.

4010 Number of data packets exceeded MAXVTAMSENDQ.

A data packet in Telnet is created when an end-of-record indicator is received. Then, the data packet is sent to the host application or is queued if the application cannot accept the data. In this case, the queue count exceeded the value coded on the MAXVTAMSENDQ statement or it exceeded the default value. A probable cause is an application that is not receiving data is stalled. Determine why the host application is not receiving data.

4011 Negative response from client received.

This special case occurs when the original BIND sent to the client does not allow exception responses. Most clients require that a BIND that is received allows exception responses. To avoid numerous connection drops, Telnet adds an exception response to the bind if one is not already specified. In this case, an exception response was returned from the client. Telnet knows that the application is not able to handle the exception and ends the session. Determine why the client found exception with the data it received.

4012 Invalid Send attempted while negotiating conn.

This special case occurs when a VTAM send request is attempted before negotiation complete. The client is usually a line-mode client that sends a carriage return or line feed before the negotiation is complete. The client will be disconnected.

4013 SNA sense error.

SNA sense data was expected in the data from the client, but the data length was not long enough to contain the SNA sense code.

4014 Client negotiation loop detected.

This special case occurs when a given client loops sends the same negotiation command to the Telnet server. The client will be disconnected. Use a client trace or DEBUG TRACE to identify the command that is repeated and determine why the client is in a negotiation loop.

4015 Client Sending in multiple USS/SOL messages.

This case occurs when a client starts sending many USS or Solicitor inputs in a single packet. This can cause severe server stalls or overhead. This return code serves as a hot IO detection for USSMSG or Solicitor processing. Use a client trace to identify the command that is repeated and determine why the client is in a loop. The client is disconnected.

4016 MAXRUCHAIN exceeded for session

The host application has exceeded the number of RUs specified by the MAXRUCHAIN value before ending the current RU chain. Modify the application to send a smaller RU chain or increase the MAXRUCHAIN value.

4017 TVLU not found

This special case occurs when a SNA BIND is received following a CLSDST PASS and the corresponding Telnet LU cannot be located. A probable cause is that Telnet LU cleanup is occurred at the same time that the BIND was received. If the problem persists, contact the IBM software support center.

4018 Amount of data exceeded MAXTCPSENDQ

When data arrives at Telnet from VTAM, the storage is queued for delivery to the client. This return code is set if the amount of storage queued exceeds the value specified by MAXTCPSENDQ. A probable cause is an application sending data to the client too quickly.

5001 Invalid TN3270E function code while negotiating.

The client is requesting an TN3270E function code that is not valid during function negotiation. Change the client so that it does not request the function that is not valid. Use a client trace or DEBUG TRACE to determine which invalid function codes are being requested.

5002 Invalid TN3270E function during negotiation.

The client is requesting an invalid TN3270E function that is not valid during function negotiation. Use a client trace or DEBUG TRACE to determine which invalid function is being requested.

5003 Printer negotiation does not allow SCS or DATA.

During connection negotiation with a printer, neither SCS nor DATA datatypes were negotiated. The client must support at least one of these datatypes to accept printer data from Telnet.

5004 WILL or DO command request rejected.

A Telnet command request from the client is unknown to the server and will be rejected. The PARM1 value is either the WILL (X'FB') command or the DO (X'FD') command and the PARM2 value is the option code.

5005 End-of-Record negotiation option failed.

A failure occurred during negotiation. Contact the IBM software support center.

5006 Transmit Binary negotiation option failed.

A failure occurred during negotiation. Contact the IBM software support center.

5007 Terminal being taken over is inactive.

A probable cause is that the original LU is deactivated. Issue an INACTLUS display command to confirm that the LU is not active.

5008 An unknown TN3270E subnegotiation detected.

An unknown TN3270E subnegotiation was received from the client. Use a client trace or DEBUG TRACE to determine which subnegotiation is in error.

5009 An unknown negotiation error was detected.

A negotiation error was detected by Telnet but is not a known error type. Use a client trace or DEBUG TRACE to determine which negotiation command is in error.

500A An unexpected new environment command detected.

An unexpected command for the new environment function was received from the client. Use a client trace or DEBUG TRACE to determine what negotiation command is in error.

500B An invalid TN3270E command detected.

An invalid TN3270E command was received from the client. Use a client trace or DEBUG TRACE to determine which negotiation command is in error.

500C An invalid SSL takeover attempt detected.

An end user is attempting a takeover of a connection that uses SSL. The new connection does not use SSL. The takeover will be ended and the client disconnected.

500D Telnet Server does not support TN3270 printer.

A client connected with a TN3270 connection type is trying to emulate a printer. This event is not supported by Telnet. Only TN3270E connections can support printer emulation. The client is disconnected.

6001 SSL/TLS failure while getting client ID.

Get ClientID request failed during SSL processing. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code from the get clientid request. Contact the IBM software support center.

6002 SSL/TLS handshake failed.

The SSL handshake with client failed. The PARM1 value is the hexadecimal error return code and the PARM3 value is the function. If the return code that you receive is not listed below or if you cannot determine the cause of the failure, see z/OS Cryptographic Services System SSL Programming. These SSL function return codes are listed as decimal values in z/OS Cryptographic Services System SSL Programming and are passed to Telnet by System SSL. The key ring file name is case sensitive. When adding the key ring name to the Telnet profile, be sure that you use the correct case. If KEYRING SAF was specified in the TN3270 profile, ensure that the TN3270 server has access to the IRR.DIGTCERT.LISTRING resource in the FACILITY class.

If PARM1 is one of the following values, try the appropriate action before calling the IBM software support center.

108 (X'6C')	The System SSL library (SGSKLOAD) could not be loaded. Ensure that TCP has access to this library.
401 (X'191')	The certificate is expired.
402 (X'192')	None of the encryption algorithms requested by the client are supported for this port.

If the ENCRYPT block is coded in the TELNETPARMS block, verify that all necessary algorithms are included. Ensure that the correct level of client code is installed on the client.

403 (X'193')

A valid server certificate was not found. If KEYRING SAF was specified in the TN3270 profile, do the following:

- Ensure that the server and signer certificates in the key ring are defined as trusted.
- If the key ring includes certificate authority or site certificates, ensure that the TN3270 server has control access to the IRR.DIGTCERT.LIST resource in the FACILITY class.
- If the certificates were added with the ICSF option, ensure that appropriate access was given to the CSFSERV resources.

405 (X'195')

The certificate type is not supported.

410 (X'19A')

An SSL message was incorrectly formatted. The following are some situations that might cause this error:

- If you are using client authentication, the client certificate was rejected during the SSL handshake. Possible problems are: The certificate expired, the certificate is not issued by a trusted CA, the certificate is in the Certificate Revocation List (CRL).
- If you are using client authentication, this message might occur if the certificate is not immediately available to the client. The client will reconnect when the client certificate is available.

414 (X'19E')

The certificate is not valid.

420 (X'1A4')

The connection was closed by the peer. If you are using client authentication, some clients disconnect when the server requests the client certificate and will reconnect when the client certificate is available.

428 (X'1AC')

No key was found for the server certificate.

437 (X'1B5')

All data has been sent by the client and no more data will be sent. The connection will be closed.

For other errors, see z/OS Cryptographic Services System SSL Programming.

6003 SSL/TLS client authentication failed.

Client authentication was requested but the client did not provide a valid certificate. Either the client did not provide a certificate or the server does not consider the client certificate to be valid. The certificate of the CA that issued the client certificate must be in the key ring of the server and must be trusted. Also, ensure that the client certificate is not expired. PARM1 might contain the system

security return code for the handshake. The PARM3 value might contain the function that was being processed when the error occurred.

6004 SSL/TLS initialization failed.

The system security interface task is not initialized. Look for an earlier DEBUG message to determine why the system security initialization task failed.

6005 SSL/TLS READ failed.

An error occurred while system SSL was reading data. The PARM1 value is the return code. Contact the IBM software support center.

6006 SSL/TLS Give Socket failed.

The give socket process failed during the SSL/TLS handshake. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code from the give request respectively. Contact the IBM software support center.

6007 SSL/TLS Take Socket failed.

The take socket process failed during the SSL/TLS handshake. The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code from the take request respectively. Contact the IBM software support center.

6008 SSL/TLS SEND failed.

An error occurred during a send request. The PARM1 value is the return value and the PARM2 value is the return code. The PARM3 value might contain the reason code. Contact the IBM software support center.

6009 SSL/TLS userid mismatch.

On takeover reconnect, the user ID associated with the client certificate did not match the original value.

600A SSL/TLS client authentication mismatch.

A takeover reconnect was attempted with a reduced CLIENTAUTH level. Ensure that the correct level of client code is installed on the takeover client.

600B SSL/TLS invalid negotiation subcommand.

During negotiated SSL/TLS, a subcommand other than StartTLS_Follows was received. The protocol used by the client might not match that used by the server. Use a client trace or DEBUG TRACE to verify that the client is using the correct SSL negotiation.

600C SSL/TLS unexpected negotiation command.

A StartTLS_Follows subcommand was received but negotiated SSL/TLS had not been requested by the server. The protocol used by client might not match that used by the server. Use a client trace or DEBUG TRACE to verify that the client is using the correct security negotiation.

600D Negotiated SSL/TLS rejected by client.

The negotiated SSL/TLS is rejected by the client. The Telnet server attempted to negotiate SSL/TLS but the client responded with a WONT STARTTLS message. The CONNTYPE for this connection is SECURE or NEGTSECURE. Because a secure connection is required and the client did not attempt to enter an SSL connection, the connection is closed.

600E SSL/TLS handshake timed out.

The time required for the client to respond to the handshake request exceeded the value coded on the SSLTIMEOUT statement or it exceeded the default. This might be expected if CONNTYPE SECURE is specified for the connection and the client uses the negotiated security protocol. Otherwise, increase the time to wait or determine why the client is not responding quickly enough.

600F System SSL initialization failed.

The setup of the security interface task failed. Secure ports will not be available, but basic Telnet is available. The Telnet interface task was set up, code began to run, but an error occurred during initialization. The PARM1 value is the hexadecimal security task return code. If the return code in

PARM1 you receive is not listed below or if you cannot determine the cause of the failure, see z/OS Cryptographic Services System SSL Programming. These SSL function return codes are listed as decimal values in z/OS Cryptographic Services System SSL Programming and are passed to Telnet by System SSL. The key ring file name is case sensitive. When adding the key ring name to the Telnet profile, be sure that the correct case is used. If KEYRING SAF was specified in the TN3270 profile, ensure that the TN3270 server has access to the IRR.DIGTCERT.LISTRING resource in the FACILITY class.

If PARM1 is one of the following values, try the appropriate action before calling the IBM software support center.

102 (X'66')

Key ring file I/O error. The cause of the error can be one of the following:

- Unable to read the key ring file required for secure communications
- Secure communications cannot continue

Verify that the z/OS UNIX file system is operating correctly and ensure that the file permissions on the key ring file are correct.

103 (X'67')

Key ring file bad format. The cause of the error can be one of the following:

- The key ring file format is incorrect
- Secure communications cannot continue

Ensure that the key ring file is correct.

201 (X'C9')

Key ring file bad password. The cause of the error can be one of the following:

- The password is incorrect or no stash file is found.
- Your cryptography hardware and ICSF are active but the TCP user ID was not given access to the RACF CSFSERV class resources.

Ensure that a stash password file was created. If the password was changed recently, ensure that the stash file was re-created. If cryptography hardware is installed, ensure that TCP was permitted to the RACF CSFSERV resources.

202 (X'CA')

Key ring file open failed. The cause of the error can be one of the following:

- Unable to open the key ring file or the key ring password stash file, which is required for secure communications. If the CRLLDAPSERVER option is specified, the LDAP server might not be accessible.
- Secure communications cannot continue.

Verify that the z/OS UNIX file system is operating correctly. If a z/OS UNIX key ring is used, verify that the stash file is in the same directory as the key ring file. If the key ring

	file is an MVS data set, verify that the stash file is also an MVS data set. Ensure that the file permissions on the key ring file are correct. Verify that the LDAP server, if specified, can be accessed from this stack.
401 (X'191')	The default certificate in the key ring file has expired or is outside the valid date range. The cause of the error might be that the default certificate in the key ring file is no longer valid. Refresh the certificate in the key ring file.
408 (X'198')	See return code 201(X'C9').
428 (X'1AC')	No private key. The cause of the error might be that the private key for the server certificate is not in the key ring file. Ensure that the key ring contains both the server certificate and private key.

For other errors, see z/OS Cryptographic Services System SSL Programming.

6010 Attach of the security interface task failed.

The MVS macro, ATTACH, failed to attach the SSL task during Telnet initialization. The PARM1 value is the ATTACH return code. Contact the IBM software support center.

6011 The security interface task has ended in error.

The security interface task ended as the result of an error condition. Instance 01 indicates that the task was set up correctly and at some later time, an error occurred. The PARM1 value is the interface task return code. Instance 02 indicates that the task was set up, but the interface task code never ran. The PARM1 value is a system completion code. The SSL task will be reattached up to three times in 10 minutes. See message EZZ6005I for the status of the reattachment. If it still fails, new connections cannot initialize for SSL. Failure might also indicate that the task was set up, the interface task code was initialized, but an error quickly occurred. The PARM1 value is the interface task return code. Contact the IBM software support center.

6012 ISTENINI could not be loaded.

The ISTENINI module used by TN3270 security support could not be loaded. The PARM1 value is the return code from the LOAD. Ensure that ISTENINI is accessible and APF authorized. Secure ports will not come online. Basic ports are not affected.

6013 CEEPIPI environments could not be initialized.

The CEEPIPI environment used by TN3270 security support could not be initialized. The PARM1 value is an additional internal return code useful to IBM Support. Secure ports will not come online. Basic ports are not affected. Contact the IBM software support center.

6014 CEEPIPI environments could not be expanded.

The CEEPIPI environment used by TN3270 security support could not be expanded. The PARM1 value is an additional internal return code useful to IBM Support. There are more encryption requests than the current C environments created by Telnet can handle. Processing will continue, but response time might be degraded. The most probable reason additional CEEPIPI environments could not be increased is that the required storage is not available.

6015 SSL/TLS HANDSHAKE WRITE complete not immediate.

The system SSL write command during the HANDSHAKE process is issued asynchronously. Because this process is running in TCB mode, a SUSPEND command cannot be issued without

blocking all other handshake processes. Ensure that the stack buffer size is at least 1024 bytes to prevent this. The session setup will fail and disconnect the client.

6016 Passticket could not be obtained.

An attempt to obtain a Passticket from RACF failed for an Express Logon macro. The PARM1 value is the SafRC from RACF, if it is available. Contact the IBM software support center.

6017 The Telnet SSL task abended.

An abend occurred in EZBTTSSL. The function will attempt to recover without the abend. The connection being processed might be disconnected with this reason code. If three failures occur in 10 minutes the task will end. See message EZZ6035I return code 6011 for a possible reason. If possible, the task will then be reattached. Look for message EZZ6005I for more information. If the problem continues, contact the IBM software support center.

6018 The Client initiated a second SSL/TLS handshake.

A client using a secure connection is in session with the SSL/TLS handshake complete. The client initiates another handshake request. The Telnet server does not support this condition. The client is disconnected.

6019 SSL handshake after SSL handshake expired.

An SSL handshake header was encountered after the SSL handshake expired. Increase the setting for the SSLTIMEOUT parameter or determine why the client is not responding quickly enough.

601A Available return code.

This return code is not used and is available for future use.

601B Available return code.

This return code is not used and is available for future use.

601C Available return code.

This return code is not used and is available for future use.

601D Available return code.

This return code is not used and is available for future use.

601E Available return code.

This return code is not used and is available for future use.

601F KEYRING is required on a Secure Port.

A secure port was defined in TelnetParms but the KEYRING option was not specified in either the TelnetGlobals statement or the TelnetParms statement.

6020 The KEYRING name is invalid.

The name might be different from the name used with current active profiles. Use the profile display command to determine whether a key ring is defined. The name might not be valid because it is different from the one already accepted for the profile that is being processed.

6021 The SSL parameter is invalid on non-Secure Port.

SSL parameters are not valid on basic ports. It is assumed that the port was meant to be secure because of the SSL parameter specified. If it is intended to be basic, remove the SSL parameter.

6022 The SSL Encryption value is invalid.

The SSL Encryption value contained in the PARM3 value is not valid compared to the values supported by the SSL subsystem. These values can be identified by displaying the Telnet defaults using the object display and specifying ID=*DEFAULT.

6023 The Encryption statement has no valid values.

All values specified are not valid or no values were specified. At least one valid value must be specified to allow the profile to process successfully.

6024 KEYRING type SAF specified but SAF unavailable.

The KEYRING statement was specified a SAF name but the secure access facility is not available. Ensure that the SAF product (such as RACF) is available and reprocess the profile.

6025 ClientAuth SAF specified but SAF unavailable.

The ClientAuth statement specified SAFcert but the secure access facility is not available. Ensure that the SAF product (such as RACF) is available and reprocess the profile.

6026 ClientAuth SAF specified but SAFcert unavailable

The client authentication portion of the secure access facility is not available. Basic SAF might be available even when the client authentication is not available. Ensure that client authentication is available and reprocess the profile.

6027 Global SSL Parm ignored on basic/TTLS port.

Global SSL parameters cannot sift down to basic ports. To avoid this message when a mixture of basic and secure ports are defined, specify the SSL parameters in the TelnetParms blocks instead of in TelnetGlobals.

6028 ParmsGroup SSL Parm ignored on basic/TTLS port.

SSL parameters have no affect on basic ports and are ignored in ParmsGroup statements. If the BeginVtam block defines both basic and secure ports the message can be avoided by splitting the BeginVtam block into two blocks, one for basic and one for secure. If the BeginVtam block defines only basic ports, remove the SSL parameters.

6029 The CRL LDAP SERVER name is invalid.

The CRL LDAP server name is not valid because a CRL LDAP server with a different name was already defined for active profiles. To change the name, deactivate all secure ports and then process the new profile with the new CRL LDAP Server name.

602A The CRL LDAP does not have a keyring.

The CRL LDAP server is used with secure connections, which requires the specification of a key ring. To use the CRL LDAP server, process a new profile with a valid key ring.

602B The SSL task initialization failed.

The Telnet task that supports SSL did not initialize. The PARM1 value is the initialization return code. Contact the IBM software support center.

602C An SSL takeover attempt was rejected.

Previous I/O to the original connection is in progress. The takeover will be aborted and the client disconnected.

602D An HSNOTIFY ioctl call failed.

A warning message will be issued for the pending connection.

602E MFA CTC token could not be obtained

An attempt to obtain a Multi-Factor Authentication (MFA) Cached Token Credential (CTC) from RACF failed for an Express Logon macro. The PARM1 value is the SAF return code, the PARM2 value is the RACF return code, and the PARM3 value is the RACF reason code. Contact the IBM software support center.

7001 Invalid character entered on logon panel.

After translating input to upper case a character that is not valid is found. See PARM1 for the hexadecimal value of the character that is not valid.

7002 Load of the default USS table failed.

The default USS table could not be loaded. The most probable cause is that it is no part of the system library is accessible to Telnet. PARM1 might contain the system completion code and PARM2 might contain the reason code. If the load module is accessible to Telnet, contact the IBM software support center.

7003 The default USS table header is an invalid type.

The USS table must be assembled with FORMAT=DYNAMIC using VTAM macros from V4R1 or later. The USS table must have a control block the ID of BD to be valid. If the IBM default USS table is being used, contact the IBM software support center.

7004 Storage for USS/INTERPRET/LUEXIT table failed.

The storage needed to manage or to save the table was not obtained. Increase storage availability. The PARM1 value is the hexadecimal amount of storage requested.

7005 The MVS LOAD of the USS/INTERPRET/LUEXIT failed.

The LOAD of the table or exit failed. The PARM1 value is the reason code of the load failure.

7006 The MVS BLDL of the USS/INTERPRET/LUEXIT table failed.

The specified table or exit was not found. The PARM1 value is the value returned by the MVS BLDL macro in R15. See z/OS DFSMS Macro Instructions for Data Sets for information about the MVS BLDL macro. This probably occurred because the table is not in a data set accessible by TCP/IP.

7007 The internal USS table type is invalid.

The table being loaded does not have the correct table identifier of BD or it was not assembled with FORMAT=DYNAMIC using VTAM macros from V4R1 or newer.

7008 The internal INTERPRET table type is invalid.

The table being loaded does not have the correct table identifier of BE. The table is not an INTERPRET table.

7009 No sequence match of input by interpret table.

Input data was passed to the interpret table but did not match any of the sequences in the table. This event is a valid situation and the input data will be processed by the USS table.

700A The returned NQN is in an invalid format.

The interpret table exit routine returned a network qualified name with a format that is not valid. Valid format is *name.network* where *name* and *network* are each a maximum of eight characters.

700B The LU/PRT exit failed the function call.

The LU/PRT exit was invoked with a specific function call. The exit failed the request with a nonzero return code. When the function is ASSIGNLU, the client connection request is ended. The PARM1 value is the return code from the LU exit. The PARM2 value is the specific function call. The PARM3 value is the name of the LU exit. If this error is unexpected, investigate the LU exit to determine the reason for rejecting the requested function.

700C The LU/PRT exit input parameters were changed.

The parameters for an LU or PRT group exit were changed. When the exit is activated, the input parameters are not allowed to be changed. This error was detected during VARY TCPIP,,OBEYFILE file processing.

700D The LU/PRT exit has been disabled due to abends.

The LU or PRT exit was disabled. The exit is disabled because it exceeded the maximum number of abends allowed for a user exit. This abend threshold is set at a maximum of three abends in a 10-minute period. Investigate and correct the root cause of the LU/PRT exit abends.

700E Calling LU/PRT exit.

The Debug trace option was selected, causing trace messages to occur. This debug message displays the contents of the parameter list being passed to the LU/PRT exit at invocation time.

700F Return from LU/PRT exit.

The Debug trace option was selected, causing trace messages to occur. This debug message displays the contents of the parameter list upon return from the LU/PRT exit invocation.

7010 LU/PRT exit not allowed with associated printer.

When an associated printer is coded on an LUMAP statement, neither the LU group or PRT group is allowed to be defined as an exit. The LUMAP statement is ignored.

7011 LU name required for LU Exit in MLS environment.

The LU Exit is required to have an LU Name or LU Range defined in the TCPIP Profile to identify a single LU, which will be the Security Standard for the LU Group in a multilevel security environment.

7012 The USS table has a type mismatch.

The USSTCP statement has an SCS or USS3270 table name that has already been added as the other type. Check your profile source and correct the names. The USSTCP can now have USSTCP *table1*,*table2* where *table1* is a USS3270 type table, and *table2* is an SCS format USS table. The statement is ignored.

7013 A Solicitor screen cannot be sent to a printer.

Telnet attempted to send a solicitor screen to a printer, but a printer cannot accept this screen. A probable cause is that a RESTRICTAPPL is being used, and ALLOWPRINTER was not coded.

7014 LU Exit specified SCS table without 3270 table.

Neither the LU exit nor the USSTCP mapping statement allows an SCS format table to be specified without a valid 3270 format table also being specified. In this case, the LU exit is trying to assign an SCS table without having a 3270 table. Change the exit or create a mapping statement to provide a 3270 format table.

7015 A table specified by the LU Exit is not loaded.

The LU exit returned a USS or Interpret table name that is not valid because the load of the table failed earlier. The connection will continue. If either the 3270 or SCS format table is not valid as a result of a load failure, neither table will be used and either the profile-mapped USS table or the solicitor panel will be used. The *PARM2* value specifies the table name that is not loaded.

7016 Incorrect USSMSG length field value.

A USSMSG was to be issued to the client, but the USSMSG in the table was defined with a length of 0.

8001 Available return code.

This return code is not used and is available for future use.

8002 Configuration task setup failed.

The setup of the Telnet configuration task failed. Without the configuration task, Telnet cannot receive any profile statements or operator commands. The PARM1 value is the configuration task return code. Contact the IBM software support center.

8003 Attach of the Configuration task failed.

The MVS macro, ATTACH, failed to attach the Configuration task during Telnet initialization. Without the configuration task, Telnet cannot receive any profile statements or operator commands. The PARM1 value is the ATTACH return code. Contact the IBM software support center.

8004 The Configuration task has ended in error.

The Configuration task ended because of an error condition that caused three abends in a 10-minute period. Without the configuration task, Telnet cannot receive any profile statements or operator commands. Contact the IBM software support center.

8005 Available return code.

This return code is not used and is available for future use.

8006 Incomplete profile update aborted for this one.

An earlier profile process that did not finish because an error is ended without being applied. The new profile request is processed. It is uncommon to end a profile in progress. If the problem persists, contact the IBM software support center.

8007 No IP mask exists for the delete request.

The IP subnet mask entry is being deleted but the IP mask cannot be found. Data corruption is the probable cause. If the problem persists, contact the IBM software support center.

8008 An AbendTrap has already been set.

A VARY AbendTrap command was already issued setting the Abend Trap. Use the Profile display command to see what is set. If you want to change the trap, turn off the current trap by specifying "OFF" as the module name and then set the new trap.

8009 Unknown display request code.

Internal processing created an incorrect display request code. This should not occur. If the problem persists, contact the IBM software support center.

800A Invalid Profile specified on Display command.

The profile number or type specified on the DISPLAY command is invalid. Issue the command with a valid profile number or no profile number.

800B Invalid DEBUG command option.

A DEBUG option other than OFF was specified. OFF is the only valid command option now.

800C Ending profile processing but none in progress.

Telnet received an "end profile" command from the TCP/IP Configuration task but no profile process was in progress. This should not occur. If the problem persists, call the IBM software support center.

800D No port match for VARY command.

The port number, range, or type specified does not match any active port. Reissue the command with an active port.

800E No port specified but multiple ports exist.

The VARY command requires that a port number, range, or type be specified if more than one port is active. Without a port specified, it is unclear whether all ports were meant to be affected.

800F No ports active for VARY command.

There are no ports active in Telnet now. The command has no affect.

8010 Unknown profile statement SubType encountered.

Internal processing created an unknown profile statement SubType. The PARM1 value is the invalid subtype. This should not occur. If the problem persists, contact the IBM software support center.

8011 Transform activation request ignored.

Transform is already active on another port and cannot be activated on this port. The original port must be deactivated before transform can be specified on this port.

8012 Invalid length received for profile statement.

An internal error caused the statement record to indicate an incorrect length for the profile statement received from the TCP/IP stack. If the problem persists, contact the IBM software support center.

8013 Invalid parameter received in profile statement.

An internal error caused the statement record to indicate an incorrect parameter for the profile statement received from the TCP/IP stack. If the problem persists, contact the IBM software support center.

8014 LUSESSIONPEND replaces QUEUESESSION.

LUSESSIONPEND and QUEUESESSION are mutually exclusive. If both are specified at any time in the profile, LUSESSIONPEND is used.

8015 QUEUESESSION ignored, already LUSESSIONPEND.

LUSESSIONPEND and QUEUESESSION are mutually exclusive. If both are specified at any time in the profile, LUSESSIONPEND is used.

8016 Invalid devicetype specified.

An invalid device type was specified on the TELNETDEVICE statement. See the TELNETDEVICE statement in z/OS Communications Server: IP Configuration Reference for a list of valid device types.

8017 Invalid 3270E devicetype specified.

An invalid 3270E device type was specified on the TELNETDEVICE statement. See the TELNETDEVICE statement in z/OS Communications Server: IP Configuration Reference for a list of valid device types.

8018 Codepage setup, including defaults, failed.

No translation tables from the specified Codepage statement or the defaults were generated. The internal Telnet translation tables will be used.

8019 Unknown profile statement ReqType encountered.

Internal processing created an unknown profile statement ReqType. The PARM1 value is the invalid ReqType. This should not occur. If the problem persists, contact the IBM software support center.

801A BEGINVTAM block with no port number.

Multiple BEGINVTAM blocks were specified in the profile. At least one block did specify a port number implying multiple ports. It is unclear which port the no-port BEGINVTAM should be matched with and is therefore ignored.

801B Multiple BEGINVTAM blocks. Last one is used.

Multiple BEGINVTAM blocks for the same port were found in the profile. The last block is used.

801C Multiple TELNETPARMS blocks. Last one is used.

Multiple TELNETPARMS blocks for the same port were found in the profile. The last block is used.

801D Multiple PORT blocks. Last one is used.

Multiple TELNETPARMS blocks for the same port were created from multiple PORT statements. The last block is used.

801E BEGINVTAM block with no TELNETPARMS block.

A BEGINVTAM block was found in the profile but has no matching TELNETPARMS block. A port definition must have both a BEGINVTAM block and a TELNETPARMS block to be successfully started or updated.

801F TELNETPARMS block with no BEGINVTAM block.

A TELNETPARMS block was found in the profile but has no matching BEGINVTAM block. A port definition must have both a BEGINVTAM block and a TELNETPARMS block to be successfully started or updated.

8020 Initialization of the Telnet Port failed.

Port activation includes attaching a load module that performs all the connection tasks. The attach or initialization of the task failed. The return code is contained in PARM1.

8021 Maximum number of Telnet Ports exceeded.

The maximum number of Telnet ports is 255. No more ports can be activated until existing ports are deactivated.

8022 Port has both secure and basic components.

The port being quiesced, resumed, or stopped has both secure and basic components. Because the port is both secure and basic, the command will not alter the port. To alter the port, reissue the command for the port without the secure or basic option.

8023 Placement accepted. Use TELNETPARMS in future.

The parameter placement in BEGINVTAM is accepted now but will have to be moved to TELNETPARMS in a future release. Move the parameter now to stop receiving the

warning message. The parameter statement can now be placed in the TELNETGLOBALS, TELNETPARMS, or ParmsGroup.

8024 Display syntax obsolete. Use OBJ/CLID display.

The display command is no longer supported in its original format. The use is accepted but is internally translated to one of the OBJect or CLient IDentifier display commands. Use the appropriate OBJect or CLient IDentifier display command to avoid this message.

8025 The Group must have less than 4294967296 LUs.

The number of LUs in the group exceeds the Telnet limit of 4294967296. Reduce the number of LUs in the group.

8026 Usage accepted but obsolete in future release.

The statement usage is accepted now but will become obsolete in a future release.

- INTERNALCLIENTPARMS - Replace with TELNETPARMS.
- QUEUESESSION - For the DEFAULTAPPLs that QUEUESESSION is affecting, add an ALLOWAPPL statement with the QSESSION option.

8027 Display syntax obsolete. Use PROF, det display.

The display command is no longer supported in its original format. The use is accepted but is internally translated to the Profile detail display command. Use that display to avoid this message.

8028 First character must be equal and not numeric.

The old style LU range requires that the first character be alphabetic or a national character (@#$) and the low entry first character must match the high entry first character. The first character might be an alphabetic range using the range rules.

8029 Variable must be all numeric or all alpha.

When no range rule is supplied, the old style LU range rule of *LUbase+LowerRange..LUbase +UpperRange* is used. It requires that the variable portion be contiguous, in the rightmost portion of the name, and entirely alphabetic or entirely numeric. If a more complex combination or variable position is required, use an explicit range rule.

802A First entry is higher than the second entry.

The first entry must be lower than the second entry to create a valid range. Ensure that the first variable column in the first entry is lower than the first variable column in the second entry. The order for Telnet LU range characters is 0-9, A-Z, @, #, $.

802B Port stop in progress. Profile update ignored.

A profile update by the VARY TCPIP,,OBEYFILE command or Telnet start was attempted for a port that is in the process of stopping. Reissue the VARY TCPIP,,OBEYFILE command after the port has stopped.

802C Variant does not match range entries.

The variant is not valid for the LU range entries specified. The range might indicate Fixed when the Start character is different from the End character or the character might not be valid for the variant specified.

802D The variant must be fixed.

The variant must be fixed for the character index. A character is the same in both the Start and End names with a variant other than Fixed with no variable character to the left. PARM1 will contain the RULE used on the LUGROUP. The letter E will appear in the position where the error was detected.

802E IPv6 address invalid in IPv4 environment.

An IPv6 format IP address was specified in the profile. Its use is not allowed in an IPv4 environment. Either change the IP address format or reinitialize the system to support IPv6 addresses.

802F TCPIP Profile Attempted to Change NACUSERID.

A NACUSERID cannot be added, omitted, or altered for an active TN3270 port in subsequent profiles. To add, omit, or alter a NACUSERID, the port must be stopped and then restarted with changes.

8030 NACUSERID profile undefined in security server.

The NACUSERID in the TCPIP profile is not defined by a security server profile.

8031 General security server error for NACUSERID.

An error was reported by the security server while attempting to create an ACEE for this NACUSERID. This error might include undefined NACUSERID profiles.

8032 FORMAT SHORT invalid in an IPv6 environment.

IPv6 addresses are potentially long and require a long print format. FORMAT SHORT is invalid in an IPv6 environment or when an IPv6 address was specified in the profile.

8033 No valid BEGINVTAM/TELNETPARMS blocks.

There are no matching BEGINVTAM/TELNETPARMS blocks to create or update a Telnet port. At least one set of BEGINVTAM/TELNETPARMS block must be present for an update to occur. A TELNETGLOBALS block by itself will update nothing because there is no port update to associate with the TELNETGLOBALS block.

8034 IP Address Range has no unique IP Addresses.

A Range was specified in an IPGROUP or DESTIPGROUP where all the addresses in its range were already accounted for by previous IP addresses and/or Ranges. Subnet Masks and Prefixes do not contribute to this error.

8035 IP Address Range failed bounds test.

A Range was specified that violates one or more of the following range bounds rules:

- Low IP less than or equal to High IP
- IPv4 Addr = xxx.xxx.xxx.nnn
- IPv6 Addr = xxxx:xxxx:xxxx:xxxx: xxxx:xxxx:xxxx:nnnn

8036 Group not added. Monitor Group table full.

The monitor group table can hold 255 unique entries. The table is full and the current monitor group will not be added to the table. Either too many groups were specified in the profile or the accumulation of monitor groups across several profiles is over the maximum. A Group is removed from the Monitor Group table when the profile defining the group is non-current and there are no active connections on the entire non-current profile.

8037 Bucket boundary value invalid.

A bucket boundary value is invalid. Bucket boundary values starting at BOUNDARY1 up to BOUNDARY4 cannot decrease in value. The PARM1 value is (in hexadecimal notation) the value in error. The PARM3 value is the parameter in error. The group is ignored. Fix the boundary value so that each value is equal to or greater than the one before it.

8038 Profile dataset failed to open.

The specified data set on the Profile DD statement or on the VARY TCPIP,,OBEYFILE command was allocated successfully but did not OPEN successfully. The PARM3 value is the rightmost 22 characters of the data set name. If greater than 22 characters, three dots (...) precede the rightmost 19 characters of the data set name.

8039 Profile dataset synchronous read error occurred.

The specified data set on the Profile DD statement or on the VARY TCPIP,,OBEYFILE command was allocated and OPENed successfully but a read buffer procedure failed. The PARM3 value is the rightmost 22 characters of the data set name. If greater than 22 characters, three dots (...) precede the rightmost 19 characters of the data set name.

803A The statement is obsolete and ignored.

The Telnet statement specified is obsolete and no longer valid. The PARM3 value is the statement that is ignored. Profile processing continues.

803B New block stmt but already in TG,TP,BV,or PG.

A new block statement was encountered while already in another block statement. The PARM2 value is the type of block being processed and the PARM3 value is the new block statement specified in error. Profile processing is ended.

803C End block received but not in that block.

A block ending statement was encountered while in a different statement block. The PARM2 value is the type of block being processed and the PARM3 value is the block ending statement in error. Profile processing is ended.

803D Entire profile process ended. No updates.

This return code is issued whenever a profile is ended because of a previous error severe enough to stop profile processing. No statements are processed. Fix the error indicated in prior debug statements and rerun the profile.

803E Parameter on command is invalid.

A parameter on the Telnet command is invalid. The command is ignored. The PARM2 value is the specific Telnet command and the PARM3 value is the parameter in error.

803F The operator command is invalid.

The Telnet command is invalid. The command is ignored. The PARM3 value is the invalid command.

8040 Parameter is not a number.

The value on the statement in the profile or command is expected to be a number but it is not. The PARM2 value is either the profile statement or the command parameter. The PARM3 value is the value specified that should have been a number.

8041 Parameter is not VTAM style format.

The value on the statement in the profile or command is expected to be a VTAM style name but it is not. The PARM2 value is either the profile statement or the command parameter. The PARM3 value is the value specified that should have conformed to the VTAM style name. See z/OS Communications Server: IP Configuration Reference in the Telnet chapter for information about BEGINVTAM and the general rules for LU naming for valid VTAM style naming convention.

8042 Required parameter missing.

A required parameter on a profile statement or a command is missing. PARM2 is the profile statement or command that is missing the required parameter.

8043 Parameter not used for this statement.

An extraneous parameter was found on a profile statement or command. The parameter is ignored and processing continues. The PARM2 value is the profile statement or command and the PARM3 value is the extra parameter that is ignored.

8044 VTAM style parameter too long.

The VTAM style name is longer than the allowed eight characters. The PARM2 value is the profile statement or command containing the invalid parameter and the PARM3 value is the invalid parameter. For profile processing, an additional message is issued indicating if the statement is usable without the invalid parameter.

8045 Parameter is not Network Qualified Name format.

The profile statement parameter should be a Network Qualified Name. A valid NQN parameter contains two valid VTAM style names connected with a period. The PARM2 value is the profile statement and the PARM3 value is the invalid parameter.

8046 Wildcard invalid for this parameter.

A wildcard format cannot be used on the specified profile statement. The PARM2 value is the profile statement and the PARM3 value is the invalid parameter.

8047 Asterisk invalid for this parameter.

The * wildcard format cannot be used on the specified profile statement. The PARM2 value is the profile statement and the PARM3 value is the invalid parameter.

8048 Parameter first position cannot be numeric.

The first position of the VTAM style parameter cannot be numeric. The PARM1 value is the first character specified, the PARM2 value is the profile statement, and the PARM3 value is the invalid parameter.

8049 Parameter longer than allowed.

The parameter specified in the PARM3 value is longer than allowed on the profile statement or command. The PARM2 value is the profile statement or command.

804A Invalid port range specified.

A Telnet command contains a PORT parameter with an invalid port range specified. The PARM3 value is the invalid PORT statement.

804B Invalid Client ID TYPE value.

The Client ID type specified on a mapping statement is not valid. See z/OS Communications Server: IP Configuration Reference in the Telnet chapter for information about BEGINVTAM and the general rules for Client IDs for valid Client ID types. The PARM2 value is the mapping statement and the PARM3 value is the invalid Client ID type and client identifier.

804C DEFAPPL parms but no DEFAPPL.

DEFAPPL parms were found on the LUMAP or PRTMAP statement but no DEFAPPL was specified. The PARM2 value is the mapping statement and the PARM3 value is the DEFAPPL parameter that is incorrectly specified. Either add DEFAPPL or remove the DEFAPPL parameter.

804D 20 or more parms is invalid for Telnet commands.

Twenty or more parameters have been specified on the command. No Telnet command has that many parameters. The command is ignored. the PARM3 value is the command being issued.

804E Capacity limit is invalid.

The capacity limit specified is outside the valid range of 0-100. The PARM2 value is the statement type and the PARM3 value is the group name and invalid range specified.

804F INCLUDE dataset loop detected.

The data set that is the target of an INCLUDE statement has been recursively included. Either the data set has an INCLUDE statement that includes itself or it includes a data set that appears earlier in the INCLUDE sequence. The PARM3 value is the last 22 characters of the data set name. If the data set name is longer than 22 characters, the PARM3 value starts with two periods (..) followed by the last 20 characters of the data set name.

8050 Groupname too long.

The Object group name is more than eight characters or the Client ID group name is more than 16 characters. The group name must be in the limits described. The PARM2 value is the group type and the PARM3 value is the invalid groupname.

8051 An LU range failed to be added to Telnet.

An internal error occurred while adding a range to the Telnet tables. The *PARM1* value indicates the group name, the *PARM3* value indicates the low and high name of the range that is in error. Contact the IBM software support center.

8052 Groupname invalid syntax.

The group name has invalid characters in it. The PARM1 value is the invalid character, the PARM2 value is the statement type, and the PARM3 value is the entire group name. See z/OS

Communications Server: IP Configuration Reference in the Telnet chapter for information about BEGINVTAM and the general rules for group name syntax.

8053 Duplicate group name. Last one is used.

One of the following occurred:

- A group name of the same type was specified more than once.
- The same group name was specified in both the LUGROUP and SLUGROUP types.
- The same group name was specified in both the PRTGROUP and SPRTGROUP types.

Use a different group name for one of the groups

8054 Invalid range rule syntax.

The range rule specified contains an invalid Character. The PARM1 value is the invalid character, the PARM2 value is the statement type, and the PARM3 value is the range in error.

8055 Invalid IP address.

The IP address does not conform to IPv4 or IPv6 format rules. The PARM2 value is the statement type and the PARM3 value is the IP address in error.

8056 Required value missing on statement/parameter.

A value is required for this statement or parameter. PARM3 is the statement or parameter that is missing the required value.

8057 Invalid hostname.

The host name that is specified does not conform to the naming rules. Either an invalid character is used or a dot is misplaced. If an invalid character is found, the PARM2 value is the invalid character. The PARM2 value is the statement type where the invalid host name is specified, and the PARM3 value is the leftmost 22 characters of the host name.

8058 Invalid label length within a hostname.

Each label in a host name must be in the range of 2-63 characters long. The PARM2 value is the statement type where the invalid host name is specified and the PARM3 value is the leftmost 22 characters of the host name.

8059 Invalid hyphen placement in hostname.

A label in the host name cannot start or end with a hyphen. The PARM2 value is the statement type where the invalid host name is specified and the PARM3 value is the leftmost 22 characters of the host name.

805A LU, LUG or USER missing.

The LU, LUG, or USER keyword was specified without an LU name or User ID following. PARM2 is the statement type containing the keyword.

805B Value outside acceptable range for statement.

The value specified is not in the range described in the z/OS Communications Server: IP Configuration Reference in the Telnet chapter. The PARM2 value is the statement in error and the PARM3 value is the invalid value specified.

805C Statement is invalid in this statement block.

A valid statement was specified in the wrong statement block. The PARM2 value is an abbreviation of the current block and the PARM3 value is the statement incorrectly placed in the block.

805D Error during read buffer process. Lost place.

An internal error has occurred while reading the profile. If this occurs, contact the IBM software support center.

805E Several unused parameters follow.

More than one unused parameter was ignored during statement processing. The PARM3 value is the second parameter. The first unused parameter was displayed in a previous debug message.

805F Invalid IP subnet.

Subnet specification is not allowed where the IP address was specified.

8060 Dataset name is in use.

The non-partitioned data set is in use and cannot be processed. Free the data set and reissue the VARY TCPIP,,OBEYFILE command. The PARM3 value is the last 22 characters of the data set name. If longer than 22 characters, the PARM3 value starts with .. followed by the last 20 characters of the data set name.

8061 Dynamic allocation of dataset failed.

The probable reason is the data set name was mistyped on the VARY TCPIP,,OBEYFILE command. The PARM1 value is the dynamic allocation return code, the PARM2 value is the reason code, and the PARM3 value is the last 22 characters of the data set name.

8062 Invalid dataset organization values.

The data set organization value is invalid. It must be either sequential or partitioned. If partitioned, a member must be specified. The PARM3 value is the last 22 characters of the data set name.

8063 Dataset name too long.

The data set name length limits for MVS, SAF, and z/OS UNIX are 44, 237, and 1024 characters, respectively. Correct the data set name and try the operation again.

8064 Statement is required on Debug Config Trace.

You must specify at least one statement name after Trace. For example, DEBUG CONFIG TRACE,LUMAP,LUGROUP

8065 Module name is required on Debug Module Trace.

You must specify at least one module name after Trace. For example, DEBUG MODULE TRACE,EZBTTCSC,EZBTVXRC

8066 Dataset name invalid.

The data set name on the PROFILE DD card does not exist, contains an invalid character or misplaced dot, or it has one of the following characteristics that are invalid for a Telnet profile data set. It is variable block or not fixed or has a record length smaller than 56 or larger than 256. Use a data set that is fixed with record length in the range of 56 - 256.

8067 Abend occurred during profile processing.

The profile process ended abnormally. Contact the IBM software support center.

8068 Duplicate statement or parameter. Last one used.

A duplicate parameter or statement was found. The last instance of the parameter or statement will be used. The specification of a statement antithesis is considered a duplicate entry. For example, MSG07 is considered a duplicate of NOMSG07. The PARM3 value is the statement or parameter being duplicated. The last value specified is the value used by Telnet. Profile processing continues.

8069 Telnet profile attempted to change affinity.

Affinity cannot be changed while Telnet is active. Telnet must be stopped and then restarted with the new TCPIPJOBNAME. PARM1 is the current stack name and PARM2 is the new name specified in the profile.

806B Maximum number of flow module names reached.

A maximum of 20 module names can be specified on a DEBUG FLOW statement. Reduce the number of names and reissue the VARY TCPIP,,OBEYFILE command.

806C Maximum number of Telnetdevice entries reached.

A maximum of 21 Telnet device statements can be specified in one Telnet block. There are 21 possible Telnet devices. Find and remove the duplicate entry.

806D Invalid TelnetParms port.

The TELNETPARMS port is invalid. The TELNETPARMS block will not be processed. An earlier DEBUG message, return code 8040, was probably issued indicating the port error.

806E Secure parm error stops secure port processing.

A security-related error reported in an earlier DEBUG message will prevent any secure port processing from completing. Telnet will not allow you to create or update a secure port if there are errors found on security-related statements.

806F Secure TelnetParms block will not be used.

A security-related error was found in the TELNETPARMS block. The entire TELNETPARMS block is ignored. Fix the error and reissue the VARY TCPIP,,OBEYFILE command.

8070 The parameter is not part of any statement.

The word found is outside a major Telnet statement block or is found after a valid END statement. PARM2 is the last valid statement processed and the PARM3 value is the invalid word found.

8071 Statement ignored. Prior values retained.

The statement in the PARM3 value was specified with an invalid value. A prior debug message was probably issued showing the error. The statement was either specified earlier in the block, or the default values were taken. The prior values will be retained for processing.

8072 Invalid optional parameter.

An invalid optional parameter was found. A second DEBUG message will indicate the disposition of the statement.

8073 All valid optional parameters are used.

A statement was found to contain at least one invalid optional parameter. All optional valid parameters, before and after the invalid parameters, are processed. The PARM3 value is the statement containing the invalid parameters. A prior DEBUG message describes the invalid parameter.

8074 Remaining optional parameters ignored.

A statement was found to contain an invalid optional parameter. All optional valid parameters up to the invalid parameter are processed. Optional parameters after the invalid parameter are ignored. The PARM3 value is the statement containing the invalid parameters. A prior DEBUG message describes the invalid parameter.

8075 Statement in error and is ignored.

The statement in the PARM3 value has a significant error and will be ignored. Remaining valid statements will be processed.

8076 Comma or position not valid with this parameter.

Use of the comma is invalid for this VTAM style name. A comma cannot be at the beginning or end of most values. Typical use of the comma is on the TELNETDEVICE or USSTCP statements. PARM2 is the statement and the PARM3 value is the value in error.

8077 Divider .. is not valid for this parameter.

Use of the .. is invalid for this VTAM style name. The .. is only valid for LU name ranges or IP address ranges. The PARM2 value is the statement and the PARM3 value is the value in error.

8078 LU low/high and range rule must be same size.

The number of characters was not the same for the low and high LU names or the range on an LU name range value. The PARM2 value is the statement containing the invalid range and the PARM3 value is the invalid range.

8079 ParmsGroup creation failed.

The ParmsGroup was not processed. See earlier DEBUG messages to see why the ParmsGroup was not processed.

807A File process ended before statement end found.

One of the Telnet statements that requires an END statement is missing the END statement. For example, LUGROUP must have ENDLUGROUP. the PARM3 value is the statement missing the END statement.

807B The Symbolics table failed to load.

The symbolics table was not loaded for Telnet use. The profile process is ended. If the problem persists, contact the IBM software support center.

807C Invalid character in SAF name.

A comma, open parenthesis [(], or close parenthesis [)] was incorrectly used in an SAF data set name.

807D Receive profile data from the dataset.

The DEBUG PROFILE option was selected, causing trace messages of data to be read in from the profile data set.

807E Send profile data to Telnet database build.

The DEBUG PROFILE option was selected, causing trace messages of data structures to be passed to the Telnet database build routine.

807F Maximum number of profile statements reached.

A maximum of 20 profile names can be specified on a DEBUG PROFILE statement. Reduce the number of names and reissue the VARY TCPIP,,OBEYFILE command.

8080 Invalid parameter on profile statement.

A parameter specified on the profile statement is not valid. The PARM2 value is the first eight characters of the profile statement containing the parameter that is not valid. The PARM3 value is the first twenty two characters of the parameter that is not valid.

8081 IP range addresses are not the same format.

When an IP address range is specified, the low and high values must be the same format, IPv4 or IPv6. Formats cannot be mixed. The PARM2 value is the statement name and the PARM3 value is the IP address range in error.

8082 IP range is invalid.

The IP range specified is invalid. The most probable cause is trying to specify a range over more than the last octet for IPv4 or more than the last two bytes for IPv6. The PARM2 value is the statement name and the PARM3 value is the IP address range in error.

8083 The ID is a different type than TYPE= specified.

The type specified was either an exact IP address or an exact host name. The ID specified is not valid for the TYPE specified. Verify that the ID is correct.

8084 TCPIPJOBNAME is not the active TCPIP stack.

The TCPIPJOBNAME does not match the active TCPIP stack. When running in an INET environment, the TCPIPJOBNAME parameter must match the jobname of the active stack. Correct the TCPIPJOBNAME and restart Telnet.

8085 User not authorized to issue this command.

The User ID attempting to issue the operator command is not authorized in the security product to issue this command.

8086 Invalid CONNTYPE stops port processing.

A CONNTYPE statement that is not valid prevents any secure port processing from completing. To prevent unintentional clear connections, Telnet does not allow you to create or update a port if the CONNTYPE statement is not valid. Correct the CONNTYPE statement and process the profile again.

8087 NOJOIN cannot be used after joining XCF group.

After a Telnet server has joined an XCF group, NOJOIN cannot be specified or used as the default. Telnet must be stopped to leave the group. Continue to specify JOIN. The entire XCFGROUP statement is ignored.

8088 The XCF group name cannot be changed.

After a Telnet server has joined an XCF group, the group name cannot be changed. Telnet must be stopped and restarted with the new name. The entire XCFGROUP statement is ignored.

8089 LUNS parm change invalid unless in QUIESC state.

The LUNS is in a state in which parameter changes are not allowed. CPARM3 specifies the parameter that is being changed. The entire XCFGROUP statement is ignored.

808A LUNS exists but missing in this XCFGROUP.

A LUNS was defined previously but is not defined in this version of the XCFGROUP. The other XCFGROUP definitions are applied and the existing LUNS remains unchanged.

808B Member of XCF group but no XCFGROUP definitions.

The VARY TCPIP,,OBEYFILE command was processed without an XCFGROUP definition in TelnetGlobals. The prior XCFGROUP definitions remain in effect.

808C The XCFGROUP is ignored. See earlier messages.

Earlier XCFGROUP warning messages reported problems with the definition, which made the XCFGROUP unusable. If prior XCFGROUP definitions were accepted, they remain unchanged.

808D The Pending profile was removed earlier.

A response from the LUNS for a LUNR pending profile failed because the profile no longer exists. The probable cause is a subsequent VARY TCPIP,,OBEYFILE command was issued, which removed the pending profile. If the problem persists, contact the IBM software support center.

808E Pending profile request failed. Port is gone.

A profile update request at the LUNS failed because the LUNS port is gone. A profile update reply at the LUNR failed because the LUNR port is gone.

808F LUNS display request invalid on non-LUNS Telnet.

You attempted to issue a LUNS display on a Telnet that is not a LUNS. Reissue the command on an XCF Telnet with an active LUNS.

8090 Shared LU groups valid only with XCF Telnet.

You attempted to specify shared LU groups on a Classic Telnet or on an XCF Telnet that failed to join the XCF group. Shared groups are not valid on non-XCF Telnet.

8091 Group name cannot be statement name.

The group name specified is a Telnet on a Classic Telnet or on an XCF Telnet that configuration statement name and cannot be used as a group name.

8094 The call to add a health check failed.

An attempt to add a Telnet health check failed.

8095 The call to delete a health check failed.

An attempt to delete a Telnet health check failed.

9001 Parms cannot be changed while subagent active.

A VARY TCPIP,,OBEYFILE command process attempted to change a subagent parameter while the subagent was active. This event is not allowed. To change a subagent parameter, the subagent must be disabled and then enabled with the new parameter value.

9002 Initialization of the Telnet subagent failed.

The attach or initialization of the Telnet subagent subtask failed. If the problem persists, contact the IBM software support center.

9003 The Telnet Subagent TNSA control block invalid.

The major control block required for the Telnet subagent is not valid. If the problem persists, contact the IBM software support center.

9004 The TSEB control block could not be found.

The required control block, EZAZTSEB, could not be located. If the problem persists, contact the IBM software support center.

9005 Setting Affinity to the requested stack failed.

The Telnet subagent could not obtain affinity to the TCP/IP stack name taken from the EZAZTSEB control block. If the problem persists, contact the IBM software support center.

9006 Unable to open a UDP socket to TCPIP.

A UDP socket is required for the Telnet subagent to communicate with the agent. A socket did not open. If the problem persists, contact the IBM software support center.

9007 The Telnet Subagent abended.

An abend occurred in the Telnet subagent. If the problem persists, contact the IBM software support center.

9008 The open packet to the agent failed.

The packet required to open the connection to the agent failed. If the problem persists, contact the IBM software support center.

9009 Parsing the connect or register packet failed.

Parsing of the data packet for connection or registration with the agent failed. If the problem persists, contact the IBM software support center.

900A No response received from open request to agent.

No response was received after sending an open request to the agent. If the problem persists, contact the IBM software support center.

900B The DPI open request failed.

The DPI open request failed for one of several reasons. For example, the agent might not be authorized or the agent identifier might be a duplicate of an already active agent. If the problem persists, contact the IBM software support center.

900C The required DPI socket could not be obtained.

The DPI socket necessary to communicate with the agent could not be obtained. If the problem persists, contact the IBM software support center.

900D The registration packet could not be built.

The packet necessary for registration with the agent could not be built. If the problem persists, contact the IBM software support center.

900E The packet received was invalid.

The packet received from the agent did not have a correct identifier in the header. If the problem persists, contact the IBM software support center.

900F There is no data for the requested connection.

The Telnet subagent attempted to obtain monitoring data for a connection that either does not exist or is not being monitored. In this case, the subagent will not report information to the agent for this connection. This event is an internal use return code. You should not see this return code in external messages.

9010 Affinity is required to start the TN subagent.

The Telnet subagent is enabled to start in Telnet running in its own address space. Affinity was not specified but is required for the Telnet subagent to know where the agent resides. Stop Telnet, set affinity using the TCPIPJOBNAME parameter, and restart Telnet.

A001 The LUNR hello is the wrong size.

A Hello received by the LUNS is the incorrect size. A packet trace can be used to determine the client. If the client is a LUNR, contact the IBM software support center.

A002 The LUNR hello is not formatted correctly.

A Hello received by the LUNS does not have the correct format. A packet trace can be used to determine the client. If the client is a LUNR, contact the IBM software support center.

A003 LUNR hello is from a LUNR unknown to the LUNS.

The LUNS cannot find the LUNR in the XCF group. PARM3 is the system name and the job name of the LUNR. Verify that the LUNR is in the same XCF group as the LUNS and the correct LUNS server address and port are coded in the XCFGROUP statement. If the problem persists, contact the IBM software support center.

A004 Tried to send data to a LUNR that is gone.

The LUNS was unable to send data to a LUNR because the LUNR left the XCF group. PARM3 is the system name and the job name of the LUNR.

A005 Send failed due to unusable connection state.

The connection between the LUNR and the LUNS is unusable. PARM3 is the system name and the job name.

A006 Telnet failed to join the XCF group.

Telnet was unable to join the XCF group name specified in the XCFGROUP statement. PARM1 contains the return code and PARM2 contains the reason code from IXCJOIN. Correct the error and refresh the Telnet configuration or restart Telnet.

A007 Telnet internal XCF services stalled.

One of the Telnet tasks that manages XCF support has stalled. PARM1 contains internal information for IBM. PARM2 indicates how many seconds the task has been hung. Review the Telnet job to ensure that Telnet is receiving enough CPU time. If the problem persists, contact the IBM software support center.

A008 The XCF User State Update failed.

Telnet was unable to update the XCF user state field using the IXCSETUS macro. PARM1 contains the return code and Parm 2 contains the reason code. Contact the IBM software support center and provide the messages and Telnet dump

A009 The LUNS or LUNR is not in a valid state.

The LUNS or LUNR has been set internally to a stat that is not valid. This condition should not occur. If you see this problem, contact the IBM software support center.

A00A Telnet is not LUNS capable. Command ignored.

A LUNS must be defined on this Telnet for the LUNS command to be accepted. Use the XCFGROUP LUNS statement to define a LUNS.

A00B LUNS accept on listener socket failed.

The LUNS received an error while trying to accept a connection on the LUNS listening socket. PARM1 contains the return code and PARM2 contains the reason code. PARM3 indicates that this was an accept failure. Review the return code and reason code and correct the error. If the problem persists, contact the IBM software support center.

A00C LUNS count ENQ failed during start.

Telnet tried to obtain an exclusive enqueue using ISGENQ. ISGENQ failed with the return code in PARM1 and the reason code in PARM2. Contact the IBM software support center.

A00D Telnet not member of XCF group. Command ignored.

Telnet must be a member of a Telnet XCF group for the display to be accepted. Specify the XCFGROUP statement to become a member of an XCF group.

A00E The LUNS/LUNR session is gone.

Telnet is unable to communicate with the LUNS/LUNR. Contact the IBM software support center if the problem persists.

A00F The LUNS/LUNR connection is gone.

The connection between the LUNS/LUNR is gone. Telnet will attempt to recover the connection. Contact the IBM software support center if the problem persists.

A010 Recovery request but LUNS not in recovery.

The LUNR attempted to send a recovery request but the LUNS is not in recovery. Contact the IBM software support center.

A011 A request did not create a request record.

Telnet was unable to make a request record. Contact the IBM software support center.

A012 LUNS is stopping during hello negotiation.

The LUNS received a Hello request from a LUNR but the LUNS is stopping. PARM3 contains the system name and the job name of the LUNR connecting to the LUNS. This event is normal if the LUNS is stopping. Otherwise, contact the IBM software support center.

A013 LUNS/LUNR send failed.

A send error occurred while trying to write on the connection between the LUNS and LUNR. PARM1 is the return code. PARM2 is the reason code.

A014 LUNS/LUNR receive failed.

A receive error occurred on the connection between the LUNS and LUNR. PARM1 is the return code. PARM2 is the reason code

A016 Requests/replies are being purged.

Telnet purged any outstanding request and replies because either the system is leaving the XCF group or the LUNR is unable to establish a connection to the LUNS.

A017 LUNR is told the hello request is invalid.

The LUNR received a response from the LUNS that indicates that the Hello sent by the LUNR was not accepted. If the LUNS is not stopping, contact the IBM software support center.

A018 The LUNR will retry the hello process.

The LUNR received a response from the LUNS, but was unable to complete Hello processing. The LUNR will try to connect to again.

A019 The member is not on the active list.

Telnet received an XCF state update but was unable to find the member as active in the XCF group. This can happen occasionally when an XCF update arrives for a member that was recently removed from the active list.

A01A This member is already on the active list.

Telnet received notification of a new active member but the partner was already active in the XCF group. Contact the IBM software support center.

A01B The XCF group exit parameter list is invalid.

Telnet received an unexpected XCF event. PARM1 is the type of event received. Contact the IBM software support center if the problem persists.

A01C The LUNR session has stopped.

The LUNS/LUNR connection stopped while either the LUNR was connecting to the LUNS or a request was being made. Contact the IBM software support center if the problem persists.

A01D The LUNS lost a start race with another LUNS.

The LUNS was unable to obtain an exclusive enqueue because another LUNS has already started. The LUNS returns to standby state.

A01E This LUNS started late and will go to standby.

The LUNS started but a newer LUNS started. The LUNS goes to standby state.

A01F The LUNS is in the wrong state for the vary cmd.

The LUNS was not in the proper state to accept the vary command. PARM3 is the command issued.

A020 The LUNR connected with incorrect count.

The LUNS received a Hello request from a LUNR, but the LUNR used an old LUNS count. The LUNR will be rejected and will try again with the correct LUNS count. Should that be LUNR?

A021 A dealloc request does not match LUNS record.

The LUNS received a deallocation request for a LU. However, the verification information did not match the information about the LUNS. Parm1 is the LU name being deallocated. Parm3 is the system name and job name of the LUNR. This error can be expected during LUNS takeover. If this message is seen at other times, contact the IBM software support center.

A022 The port no longer exists.

Telnet is unable to process a LUNS/LUNR request because the port was deleted. The request is failed.

A023 The profile no longer exists.

Telnet is unable to process a LUNS/LUNR request because the profile for this request was deleted. The request is failed.

A024 LUNR sent dealloc after recovery - LU not alloc.

Deallocs can fail because the dealloc request was built during a rebuild/recover session. When the LUNR sent the LUNS the list of alloc'd LUs, any pending dealloc requests LUs wouldn't be listed. When the LUNS goes active, these Deallocs would be sent. They will fail with A024. PARM1 is the LU name. PARM3 is the system name and job name of the LUNR. In any other scenario, this is an unexpected error - call the IBM software support center.

A026 The LUNR hello is invalid and should retry.

The LUNS was unable to accept a hello request from a LUNR. The LUNR will try the hello request again. PARM3 is the system name and jobname of the LUNR. If the problem persists, contact the IBM software support center.

A027 The LUNS port already in use as a Telnet port.

The XCFGROUP statement configured a LUNS port which is already in use as a Telnet port. A port cannot be used for both. PARM1 is the port number in hexidecimal.

A028 The Telnet port already in use as a LUNS port.

The TELNETPARMS statement configured a Telnet port that is already in use as a LUNS port. A port cannot be used for both. Parm1 is the port number in hexadecimal.

A029 Local LU takeover of shared LU is invalid.

An attempt to takeover a LU was failed because the LU is a shared LU allocated from a LUNS. The takeover request was initiated by a non-shared LU request.

A02A Telnet CPU constraint.

Telnet timer driven events are not occurring on time. The task that schedules events is not getting CPU cycles. If the reporting module is EZBTXSTA, Telnet has not updated a field monitored by XCF in more than the amount of time specified on the XCFMONITOR statement. PARM1 is set to 1 if a dump process was the reason, otherwise PARM1 is 0. PARM2 is the time, in hexadecimal seconds, since the last successful internal check. If the reporting module is EZBTXUT2, the timer driven task is running often enough to update the field checked by XCF, but is not running in a timely enough manner to determine the health of other Telnet tasks. If you see this RCODE occasionally, your system is probably near capacity. If you see this RCODE repetitively, either the system is constantly at capacity or there is a problem in Telnet. If the system is not at capacity, contact the IBM software support center.

System action

None.

Operator response

See the specific return code for the operator response. If the return code directs you to contact the IBM software support center, then take a dump of Telnet. If you can re-create the problem, obtain a CTRACE with the Telnet option.

System programmer response

See the specific return code for the system programmer response. If the return code directs you to contact the IBM software support center, then take a dump of Telnet. If you can re-create the problem, obtain a CTRACE with the Telnet option.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: Telnet

Module

EZAZMTNS

Routing code

(2,8),11

Descriptor code

(4,4)

Example

The following Debug message is issued when the DEBUG CONN DETAIL option is requested and the application name is not known to VTAM. The IP address and port of the client, the TCPIP connection identifier, LU name, and Telnet module issuing the message are supplied. The return code in this case is 2011 and the instance of the return code in this module is 00. In cases where a module issues the return code several times the instance is helpful to IBM service. A short text explanation follows the return code, which is often enough to solve the problem. The parameters are specific to each return code.

```
EZZ6035I jobname DEBUG CONN DETAIL
  IP..PORT: 9.37.215.132..4599
  CONN: 00000026  LU: TCPM1001  MOD: EZBTVXRQ
  RCODE: 2011-00  VTAM macro REQSESS failed.
  PARM1: 00000004 PARM2: 00000010 the PARM3 value: 00101200
```

Chapter 8

SNA Messages

Topics:

ISTM041I

Native TLS/SSL support is not in use by any TN3270 server on this system

Explanation

The check ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL ran successfully and found no exceptions. The check determined that none of the active TN3270 servers use native TLS/SSL support.

IBM has indicated in statements of direction that support for native TLS/SSL in TN3270 will be withdrawn in a future release of the IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

No action is needed.

System programmer response

No action is needed.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM041I Native TLS/SSL support is not in use by any TN3270 server on this
 system
```

ISTM042E

One or more TN3270 servers are using native TLS/SSL support

Explanation

The check ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL determined that one or more TN3270 servers are using native TLS/SSL support.

IBM has indicated in statements of direction that support for native TLS/SSL in TN3270 will be withdrawn in a future release of the IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Examine the report that was produced by this check. To assist in identifying the server instance, the report contains the TN3270 server *jobname* in the first column and the ASID value in hexadecimal format in the second column. The TN3270 server profile includes the SECUREPORT configuration statement.

See Converting Telnet profile statements to equivalent AT-TLS policy statements in z/OS Communications Server: IP Configuration Guide for more information.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM042E One or more TN3270 servers are using native TLS/SSL support
```

ISTM043I

Native TLS/SSL support is not in use on this system for DCAS

Explanation

The check ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL ran successfully and found no exceptions. The check determined that native TLS/SSL support is not in use on this system for the Digital Certificate Access Server (DCAS).

IBM has indicated in statements of direction that support for native TLS/SSL in DCAS will be withdrawn in a future release of the IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

No action is needed.

System programmer response

No action is needed.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM043I Native TLS/SSL support is not in use on this system for DCAS
```

ISTM044E

Native TLS/SSL support is in use on this system for DCAS

Explanation

The check ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL determined that native TLS/SSL support is in use on this system for the Digital Certificate Access Server (DCAS).

IBM has indicated in statements of direction that support for native TLS/SSL in DCAS will be withdrawn in a future release of the IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Because native TLS/SSL support in DCAS will no longer be supported in the TCP/IP profile in a future release of z/OS Communications Server, IBM suggests that customers who currently use or are planning to use native TLS/SSL in DCAS migrate to use AT-TLS in DCAS.

See Migrating the DCAS server to use AT-TLS policies in z/OS Communications Server: IP Configuration Guide for more information.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM044E Native TLS/SSL support is in use on this system for DCAS
```

ISTM045I

No active FTP servers are using native TLS/SSL support

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL ran successfully and found no exceptions. The check determined that none of the active FTP servers use native TLS/SSL support.

IBM has indicated in statements of direction that support for native TLS/SSL in the z/OS FTP server will be withdrawn in a future release of the IBM z/OS Communications server.

System action

The system continues processing.

Operator response

Not applicable.

System programmer response

Not applicable.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM045I No active FTP servers are using native TLS/SSL support
```

ISTM046E

One or more active FTP servers are using native TLS/SSL support

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL determined one or more FTP servers are using native TLS/SSL support.

IBM has indicated in statements of direction that support for native TLS/SSL in the z/OS FTP server will be withdrawn in a future release of the IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Examine the report that was produced by this check. To assist in identifying the server instance, the report contains the FTP server jobname in the first column and the ASID value in hexadecimal format in the second column.

Native TLS/SSL support for the FTP Server will no longer be supported in a future release of z/OS Communications Server. If you currently use or are planning to use native TLS/SSL for the FTP Server, migrate to use AT-TLS for the FTP Server.

See Steps for migrating the FTP server and client to use AT-TLS in z/OS Communications Server: IP Configuration Guide for more information.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM046E One or more active FTP servers are using native TLS/SSL support
```

ISTM047I

No active FTP servers are configured with TLSMECHANISM ATTLS and TLSRFCLEVEL CCCNONOTIFY

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL ran successfully and found no exceptions. The check determined that none of the active FTP servers are configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and EXTENSIONS AUTH_TLS. This combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Not applicable.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM047I No active FTP servers are configured with TLSMECHANISM ATTLS and
 TLSRFCLEVEL CCCNONOTIFY
```

ISTM048E

One or more active FTP servers are configured with TLSMECHANISM ATTLS and TLSRFCLEVEL CCCNONOTIFY

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL determined that TLSRFCLEVEL CCCNONOTIFY has been configured with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS for at least one FTP server. This combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Examine the report that was produced by ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL health check. To assist in identifying the server instance, the report contains the FTP server jobname in the first column and the ASID value in hexadecimal format in the second column.

The configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and EXTENSIONS AUTH_TLS will be rejected in a future release of z/OS Communications Server. For the FTP servers identified in the report, you should update the configuration to specify TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005. See z/OS Communications Server: IP Configuration Reference for information on the TLSRFCLEVEL parameter.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM048E One or more active FTP servers are configured with TLSMECHANISM
 ATTLS and  TLSRFCLEVEL CCCNONOTIFY
```

ISTM049I

No FTP clients configured with TLSMECHANISM ATTLS and TLSRFCLEVEL CCCNONOTIFY

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL ran successfully and found no exceptions. The check did not detect an FTP client configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and SECURE_MECHANISM TLS. This combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

Not applicable.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM049I No FTP clients configured with TLSMECHANISM ATTLS and TLSRFCLEVEL
 CCCNONOTIFY
```

ISTM050E

One or more FTP clients are configured with TLSMECHANISM ATTLS and TLSRFCLEVEL CCCNONOTIFY

Explanation

Check ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL determined that TLSRFCLEVEL CCCNONOTIFY has been configured with TLSMECHANISM ATTLS and SECURE_MECHANISM TLS for at least one FTP client. This combination is not a valid configuration and will be rejected in a future release of IBM z/OS Communications Server. See z/OS Communications Server: IP Configuration Reference for information on the TLSRFCLEVEL parameter.

The FTP client configuration has been in use on this system during this IPL. This exception will continue to be reported for the duration of this IPL, or as long as this migration health check is active. When this exception condition is detected, message ISTM050E is issued and is followed by message ISTM900I which indicates the date and time that an FTP client with this configuration was last detected.

System action

The system continues processing.

Operator response

Contact the system programmer.

System programmer response

To assist in identifying the client instances, message EZYFT79I is written to syslogd when an FTP client is detected with a configuration that includes TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS and SECURE_MECHANISM TLS. Message EZYFT79I is written to syslogd using facility local1 and priority warning. It includes the *jobname* and *userid* of the FTP client.

The configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS and SECURE_MECHANISM TLS will be rejected in a future release of z/OS Communications Server. For the FTP clients using this configuration, you should update the configuration to specify TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT. RFC 4217 was adopted as a standard in 2005. See z/OS Communications Server: IP Configuration Reference for information on the TLSRFCLEVEL parameter.

User response

Not applicable.

Problem determination

Not applicable.

Source

z/OS Communications Server Health Checker

Module

ISTHCCK2

Routing code

Not applicable.

Descriptor code

Not applicable.

Automation

Not applicable for automation.

Example

```
ISTM050E One or more FTP clients are configured with TLSMECHANISM ATTLS and
 TLSRFCLEVEL CCCNONOTIFY
```