



IBM eServer™

## IBM Configuration Assistant for z/OS® Communications Server - Example of use

@business on demand software

© 2007 IBM Corporation

## Agenda - IBM Configuration Assistant for z/OS Communications Server



1 Example use of the Configuration Assistant - TN3270 Server using AT-TLS

## The z/OS Communications Server Configuration Assistant



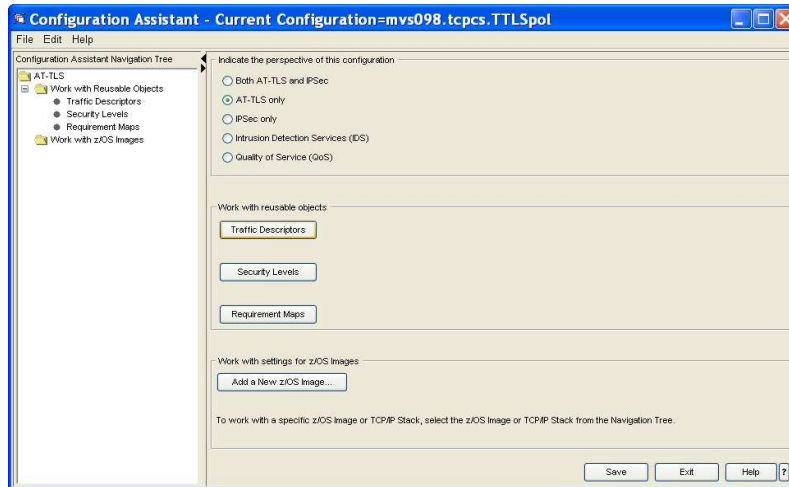
This is the consolidated policy configuration tool for CS z/OS V1R8.

In z/OS V1R8, this tool can be used to manage policies for:

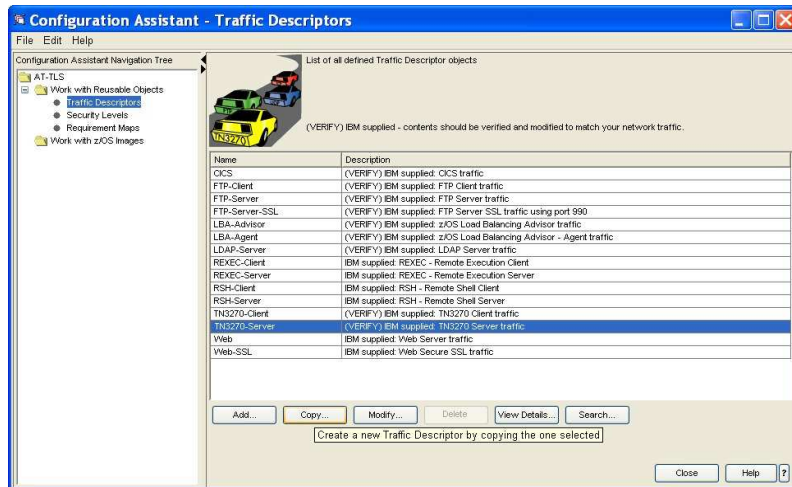
- AT-TLS
- IPsecurity
- Intrusion Detection Services (IDS)
- Quality of Service (QoS)



## Start creating a traffic descriptor



## Create a new TN3270 server port traffic descriptor by copying and modifying the sample TN3270 server descriptor



## Enter the details identifying traffic to a secure TN3270 server on port 2031

## Map the traffic descriptor to security requirements

**Requirement Map**

A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map: 1. Select a Traffic Descriptor from the Objects section.  
2. Click the "←Add" button

To change the Security Level of a Traffic Descriptor: 1. Click the Security Level column in the Requirement Map section.  
2. Select a new Security Level from the list

Requirement Map  
Name: Req-TN3270-Secure  
Description: Secure TN3270 requirements

Traffic Descriptor	Security Level
AT-TLS - Security Level	

←Add

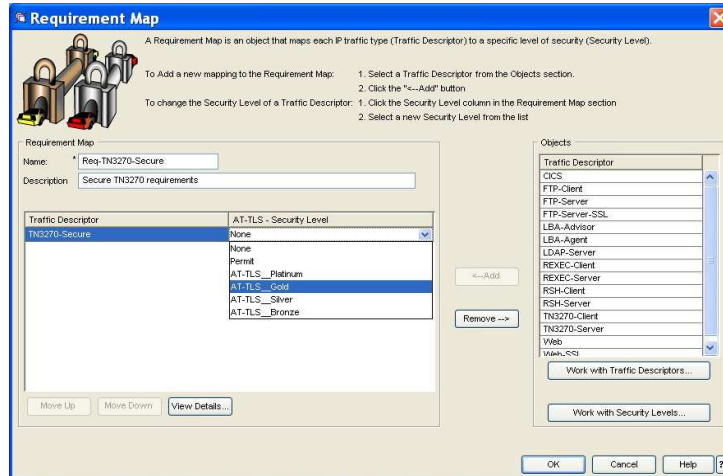
Add a new row to the table

**Security Level Objects**

List of all defined Security Level objects

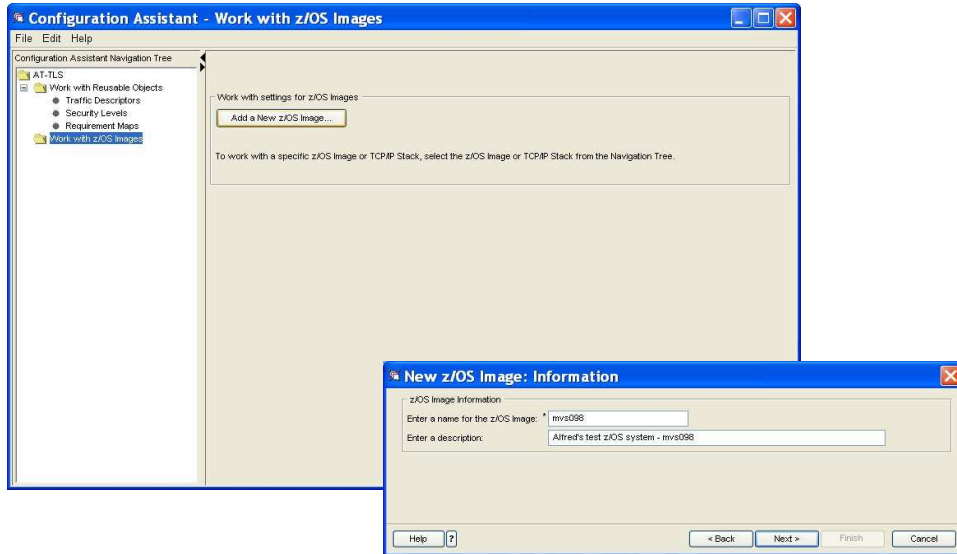
Name	Description	Cipher (First Choice)	Type
Permit	IBM supplied. Traffic is allowed with no security	None / None	No security
AT-TLS_Platinum	IBM supplied. Extremely high level of protection	x25-rsa_with_aes_256_cbc_sha	AT-TLS
AT-TLS_Gold	IBM supplied. High level of protection	x0A-rsa_with_3des_edc_cbc_sha	AT-TLS
AT-TLS_Silver	IBM supplied. Medium level of protection	x09-rsa_with_des_cbc_sha	AT-TLS
AT-TLS_Bronze	IBM supplied. Low level of protection	x02-rsa_with_null_sha	AT-TLS

## Use AT-TLS gold services for a TN3270 server





## Specify which z/OS system these policies are intended for



## Specify system-wide defaults for AT-TLS - and add stack information

The screenshot displays two overlapping dialog boxes from the IBM Configuration Assistant for z/OS Communications Server.

The larger dialog box, titled "New z/OS Image: AT-TLS Image Level Settings", contains the following sections:

- Default AT-TLS key ring database settings:**
  - Key ring database:**
    - Key ring is in SAF product (such as RACF): Key ring: [PWTEST]
    - Key database is a z/OS UNIX file system file:
      - Key database: \*
      - Key database stash file: \* or
      - Key database password: \*
- Default AT-TLS trace level:**
  - Level 0 - No tracing is enabled
  - Log only the selected trace levels:
    - Level 1 - Errors (to TCP/IP Joblog)
    - Level 2 - Errors (to Syslog)
    - Level 4 - Information (to Syslog)
- Additional AT-TLS Image settings:**
  - Advanced...

The smaller dialog box, titled "New TCP/IP Stack: Name", contains the following fields:

- TCP/IP Stack Information:**
  - Enter the name of the TCP/IP Stack: [TCPCS]
  - Enter a description: [Primary TCP/IP Stack on mvs098]

Both dialog boxes include a "Help" button with a question mark icon and a "< Back" button. The "New TCP/IP Stack: Name" dialog also includes "Next >", "Finish", and "Cancel" buttons.

## Identify the IP addresses (or ranges) that must use this requirement map

**Connectivity Rule: Data Endpoints**

Use this panel to identify the data endpoints.  
These are the IP addresses of the host endpoints of the traffic you want to protect.

**Local data endpoint**

- All IP V4 addresses
- All IP V6 addresses
- Specify address:

Syntax: Single IP V4 address: x.x.x.x  
 IP V4 subnet: x.x.x.yyy  
 IP V4 range: x.x.x.y.y.y  
 Single IP V6 address: x:x  
 IP V6 subnet: x:xyyy  
 IP V6 range: x:y:z.y

**Remote data endpoint**

- All IP V4 addresses
- All IP V6 addresses
- Specify address:

Syntax: Single IP V4 address: x.x.x.x  
 IP V4 subnet: x.x.x.yyy  
 IP V4 range: x.x.x.y.y.y  
 Single IP V6 address: x:x  
 IP V6 subnet: x:xyyy  
 IP V6 range: x:y:z.y

Connectivity Rule Name  
 Name: All-Pv4-Addresses

**Connectivity Rule: Select Requirement Map**

Select a Requirement Map  
 Initially, you need to create a new Requirement Map which will be reusable in subsequent Connectivity Rules.  
 IBM has supplied examples you can use to "Copy..." and then modify to get started.

Until you become familiar with Requirement Maps please use the **Add for Beginners...** to create your Requirement Map.

Name	Description
Req-TN3270-Secure	Secure TN3270 requirements
AT-TLS_Sample	IBM supplied: AT-TLS sample: CICS and TN3270

Buttons: Add for Beginners..., Add..., Copy..., Modify..., View Details..., Need More Information

## View and save (or FTP) the final AT-TLS policies

The screenshot displays two windows from the IBM Configuration Assistant. The left window, titled "Installation - Stack= 'TCPCS'", shows the "Configuration Files Installation" step. It lists the file "TCPCS - AT-TLS Policy Agent Stack Configuration" with columns for "File", "Sent", and "FTP". Below the table are buttons for "Show Configuration File...", "FTP...", "System Administration Information", and "Show the selected configuration file".

The right window, titled "AT-TLS Policy Agent Configuration File for Stack: TCPCS", displays the configuration file content:

```
##
## AT-TLS Policy Agent Configuration file for:
## Image: mvs098
## Stack: TCPCS
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 1 Release 8
## Date Created = Sun Jul 23 14:35:38 EDT 2006
##
## Copyright = None
##
TLSRule                               All-IPv4-Addresses-1
(
  LocalAddrSetRef                       addr1
  RemoteAddrSetRef                       addr1
  LocalPortRangeRef                       portP1
  RemotePortRangeRef                       portP2
  Jobname                                  TM3270A
  Userid                                    TCPCS
  Direction                                 Inbound
  Priority                                  255
  TLSGroupActionRef                       gAct1-TM3270-Secure
  TLSEnvironmentActionRef                 eAct1-TM3270-Secure
  TLSConnectionActionRef                 cAct1-TM3270-Secure
)
TLSGroupAction
(
  TLSEnabled                              On
)
TLSEnvironmentAction
(
  HandshakeRole                            Server
  EnvironmentUserInstance                   0
  TLSKeyringParamsRef                       keyP1
)
TLSConnectionAction
(
  HandshakeRole                            Server
  TLSCipherParamsRef                       cipher1-AT-TLS_Gold
)

```

Buttons for "Print...", "Save As...", and "Close" are visible at the bottom of the right window.

## The generated AT-TLS policies in text format

```

Session C - [43 x 80]
File Edit View Communication Actions Window Help
File Edit Edit Settings Menu Utilities Compilers Test Help
EDIT /etc/tcpcs/pagent.ttls Columns 00001 00072
Command ==> Scroll ==> CSR_
***** Top of Data *****
000001 ##
000002 ## AT-TLS Policy Agent Configuration file for:
000003 ## Image: avso98
000004 ## Stack: TCPCS
000005 ##
000006 ## Created by the IBM Configuration Assistant for z/OS Communications Se
000007 ## Version 1 Release 8
000008 ## Date Created = Sun Jul 23 14:35:38 EDT 2006
000009 ##
000010 ## Copyright = None
000011 ##
000012 TTLSRule All-IPv4-Addresses*1
000013 {
000014 LocalAddrSetRef addr1
000015 RemoteAddrSetRef addr1
000016 LocalPortRangeRef portR1
000017 RemotePortRangeRef portR2
000018 Jobname TN3270A
000019 Userid TCPCS
000020 Direction Inbound
000021 Priority 255
000022 TLSGroupActionRef gAct1^TN3270-Secure
000023 TLSEnvironmentActionRef eAct1^TN3270-Secure
000024 TLSConnectionActionRef cAct1^TN3270-Secure
000025 }
000026 TLSGroupAction gAct1^TN3270-Secure
000027 {
000028 TLSEnabled On
000029 }
000030 TLSEnvironmentAction eAct1^TN3270-Secure
000031 {
000032 HandshakeRole Server
000033 EnvironmentUserInstance 0
000034 TLSKeyparingParamsRef keyR1
000035 }
000036 TLSConnectionAction cAct1^TN3270-Secure
000037 {
  
```

## Policy agent (PAGENT) setup

```
//PAGENT  PROC P='-d 0 -c /etc/pagent.conf'
//PAGENT  EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//        PARM='POSIX(ON) ALL31(ON)
ENVAR (" _CEE_ENVFILE=DD:STDENV" )/&P'
//STDENV  DD PATH='/etc/pagent.env',PATHOPTS=(ORDONLY)
//*
//STDOUT  DD SYSOUT=*
//STDERR  DD SYSOUT=*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
//SYSOUT  DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

Policy agent start-up JCL procedure.

```
##
## pagent.conf file
##   Image: mvs098
##
TcpImage TCPCS  FLUSH 600    #Check every 10 minutes for updates
TTLSConfig /etc/tcps/pagent.ttls FLUSH PURGE
```

Policy agent start-up configuration file, which identifies the TCP/IP stack and the file name where the AT-TLS policies for that stack are stored.

## Remember the EZB.INITSTACK SERVAUTH profile before enabling TTLS on TCPConfig!

```

CLASS      NAME
-----
SERVAUTH  EZB.INITSTACK.*.* (G)

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----
00     USER1      NONE              ALTER        NO
.....

USER      ACCESS
-----
USER1     ALTER
TCPSC     READ

```

➤ When TCP/IP starts with TCPCONFIG TTLS specified, it will issue the following message

-EZZ4248E TCPSC WAITING FOR PAGENT TTLS POLICY

➤ From then on and until PAGENT has been started and installed the TTLS policies into the TCP/IP stack, the TCP/IP stack will only allow users permitted to the EZB.INITSTACK.system.stack SERVAUTH profile to establish connections.

- Make sure all your pertinent server address spaces (including PAGENT and OMPROUTE) run under user IDs that are permitted to this profile.

## TN3270 server setup when using AT-TLS

```
TelnetParms
Port 2031                ; Port number 2031 (security via TTLS)
Conntype Basic          ; Non-secure port (from TN's view)
CodePage ISO8859-1 IBM-1047 ; Linemode ASCII, EBCDIC code pages
Debug detail console
EndTelnetParms
```

When using AT-TLS, the TN3270 server does not know that connections are secured. From a TN3270 server perspective, the port is a basic non-secure port.

For scenarios where only server authentication is needed (in addition to encrypted connections), this is normally perfectly fine.

For express-logon and for scenarios where the TN3270 server maps TN3270 resources, such as LU names, based on user ID - you need to use the TN3270-specific security functions for now (z/OS V1R7 and V1R8).

```
Session D - [24 x 80]
File Edit View Communication Actions Window Help
USSMSG10: Enter: LOGON APPLID() LOGMODE() DATA()
Port: 01288 Date: 23/07/06 LU: TCPABC51
IPADDR: 9.76.141.120 Time: 14:47:48 Sense:
USSABC - This is the TCPCS Stack on MVS098

Welcome to MVS098 - Enter either full LOGON command or:
one of the following short commands:

TS0ABC - TS0 as USER1
TS012-TS018 - TS0 as USER12 to USER18
CICS - DBDCCICS on mvs098

MB d 06/001
Connected to remote server/host.mvs098o.tcp.raleigh.ibm.com using lu/pool TCPABC51 an
```



## Netstat reports include lots of good details when using AT-TLS

```

NETSTAT ALL TCP TCPCS ( CLI TN3270A

Client Name: TN3270A          Client Id: 00000DD
Local Socket: ::ffff:9.42.105.45..2031
Foreign Socket: ::ffff:9.76.141.120..1288
BytesIn:      00000000000000000032
BytesOut:     00000000000000000631
SegmentsIn:  00000000000000000015
SegmentsOut: 00000000000000000015
Last Touched: 18:47:49      State:      Establish
RcvNxt:      3791287052     SndNxt:    0996954608
ClientRcvNxt: 3791286711        ClientSndNxt: 0996952341
InitRcvSeqNum: 3791286678     InitSndSeqNum: 0996951709
CongestionWindow: 0000006968   SlowStartThreshold: 0000065535
IncomingWindowNum: 3791418087   OutgoingWindowNum: 0997020143
SndWl1:      3791287052     SndWl2:    0996954608
SndWnd:      0000065535     MaxSndWnd: 0000065535
SndUna:      0996954608     rtt_seq:   0996953929
MaximumSegmentSize: 0000000536   DSField:   00
Round-trip information:
Smooth trip time: 63.000        SmoothTripVariance: 211.000
ReXmt:      0000000000        ReXmtCount: 0000000000
DupACKs:    0000000000
SockOpt:    C000              TcpTimer:   00
TcpSig:     01                TcpSel:     00
TcpDet:     E0                TcpPol:     00
QOSPolicyRuleName:
TTLSPolicy: Yes
TTLSRule:   All-IPv4-Addresses-1
TTLSGrpAction: gAct1-TN3270-Secure
TTLSEnvAction: eAct1-TN3270-Secure
TTLSConnAction: cAct1-TN3270-Secure
ReceiveBufferSize: 0000065536   SendBufferSize: 0000065536

```

The netstat all report includes a section of AT-TLS information if the connection is secured by AT-TLS.

## Netstat TTLS report shows security details per connection

```

NETSTAT TTLS CO 0000DD DETAIL TCP TCPCS

MVS TCP/IP NETSTAT CS V1R7      TCPIP Name: TCPCS      18:55:29
ConnID: 000000DD
JobName:      TN3270A
LocalSocket:  ::ffff:9.42.105.45..2031
RemoteSocket: ::ffff:9.76.141.120..1288
SecLevel:     TLS Version 1
Cipher:       0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
CertUserID:   N/A
MapType:      Primary
TTLSRule: All-IPv4-Addresses-1
Priority:     4278190080
LocalAddr:   0.0.0.0/0
LocalPort:   2031
RemoteAddr:  0.0.0.0/0
RemotePortFrom: 1024      RemotePortTo: 65535
JobName:     TN3270A
UserID:      TCPCS
Direction:   Inbound
TTLSGrpAction: gAct1-TN3270-Secure
GroupID:      00000002
TTLSEnabled:  On
TraceClearText: Off
Trace:        2
SyslogFacility: Daemon
SecondaryMap: Off
    
```

If you need detailed AT-TLS information for a specific connection, the netstat TTLS report can be used to provide insight into lots of the details around SSL/TLS for that connection.

```

TTLSEnvAction: eAct1-TN3270-Secure
EnvironmentUserInstance: 0
HandshakeRole: Server
Keyring:        PKITEST
SSLV2:          Off
SSLV3:          On
TLSV1:          On
ResetCipherTimer: 0
ApplicationControlled: Off
HandshakeTimeout: 10
ClientAuthType: Required
TTLSConnAction: cAct1-TN3270-Secure
HandshakeRole: Server
V3CipherSuites: 0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
                 2F TLS_RSA_WITH_AES_128_CBC_SHA
    
```

## Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM                    MVS                    z/OS

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.