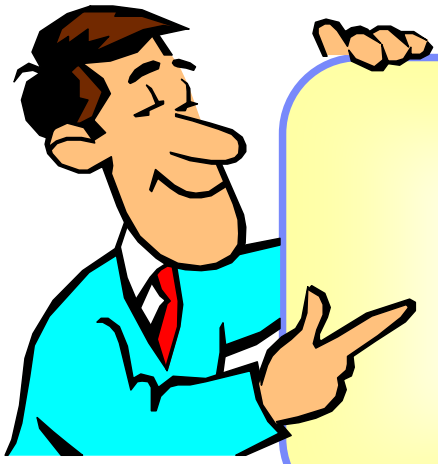
IBM eServer™

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

ebusiness on demand software

Agenda - IBM Configuration Assistant for z/OS Communications Server



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

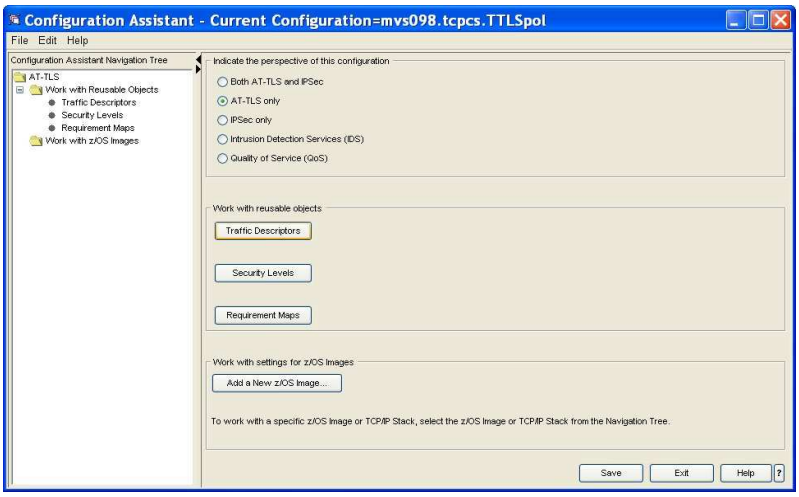
The z/OS Communications Server Configuration Assistant

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

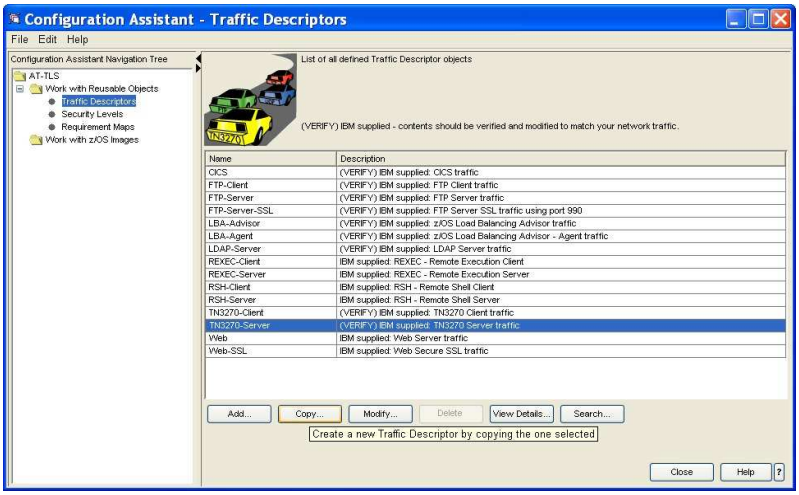
In z/OS V1R8, this tool can be used to manage policies for:

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

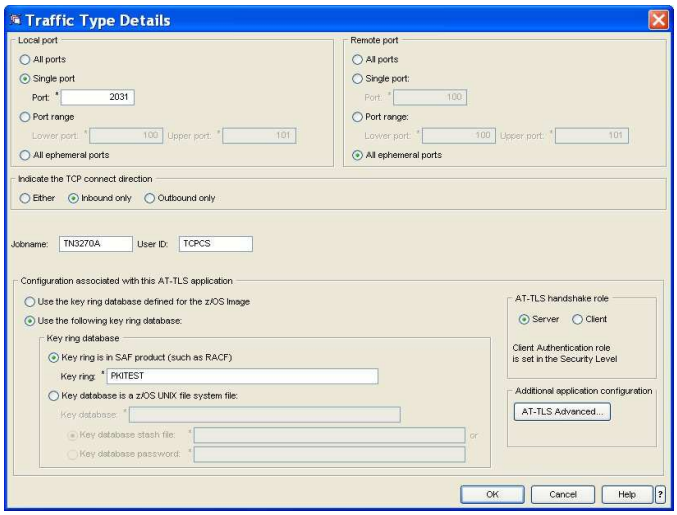
Start creating a traffic descriptor



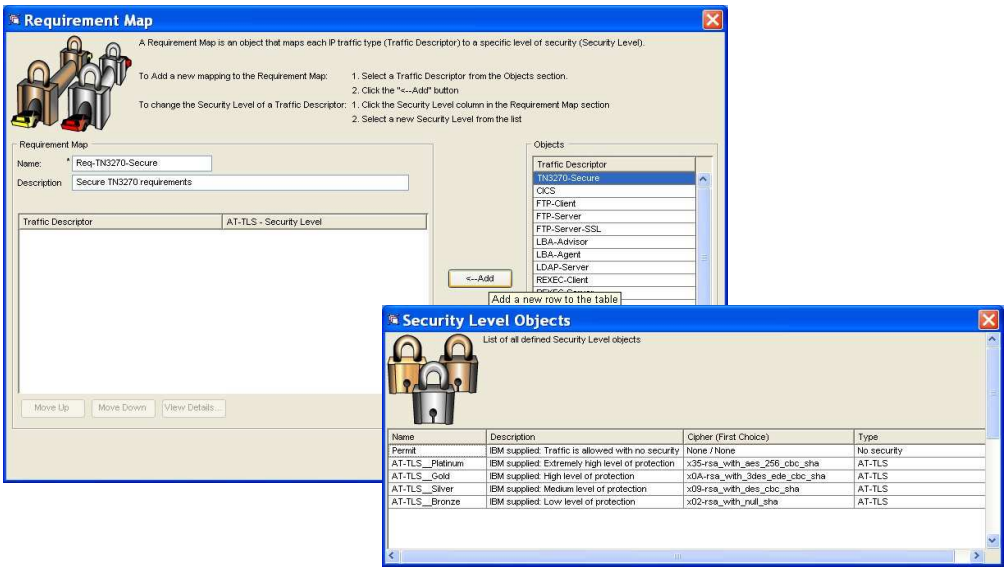
Create a new TN3270 server port traffic descriptor by copying and modifying the sample TN3270 server descriptor



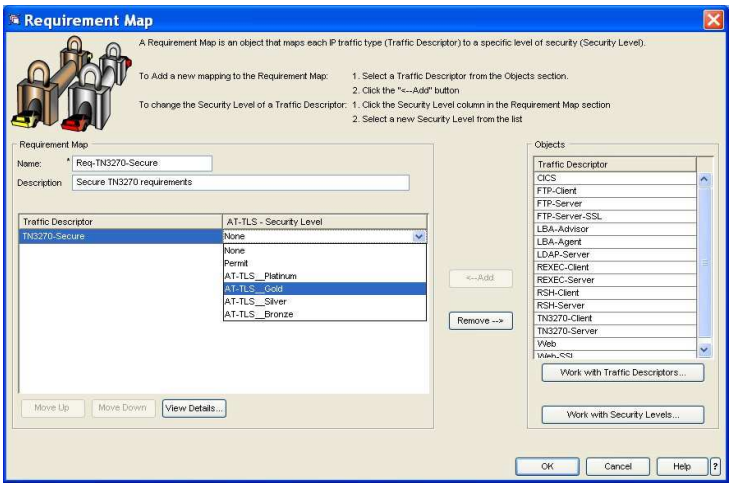
Enter the details identifying traffic to a secure TN3270 server on port 2031



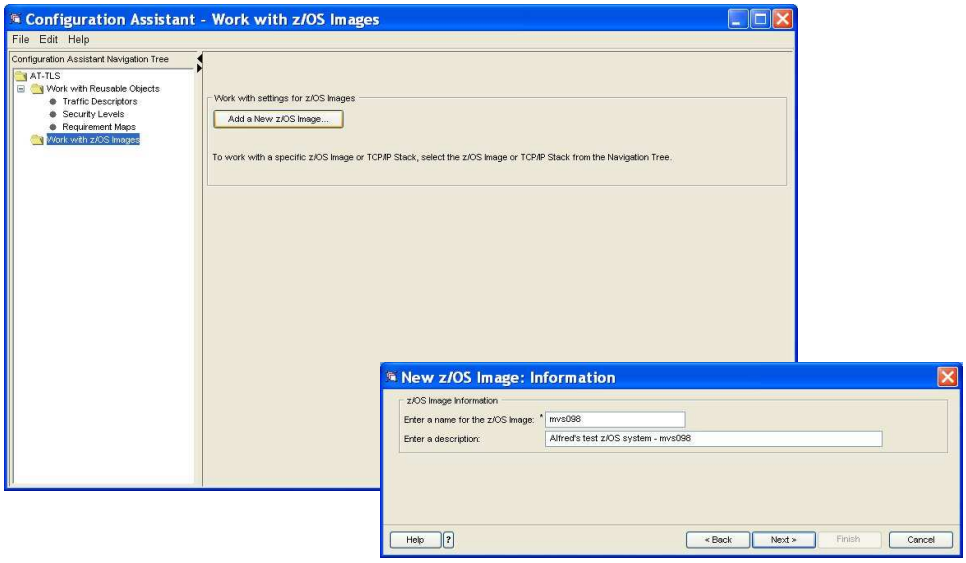
Map the traffic descriptor to security requirements



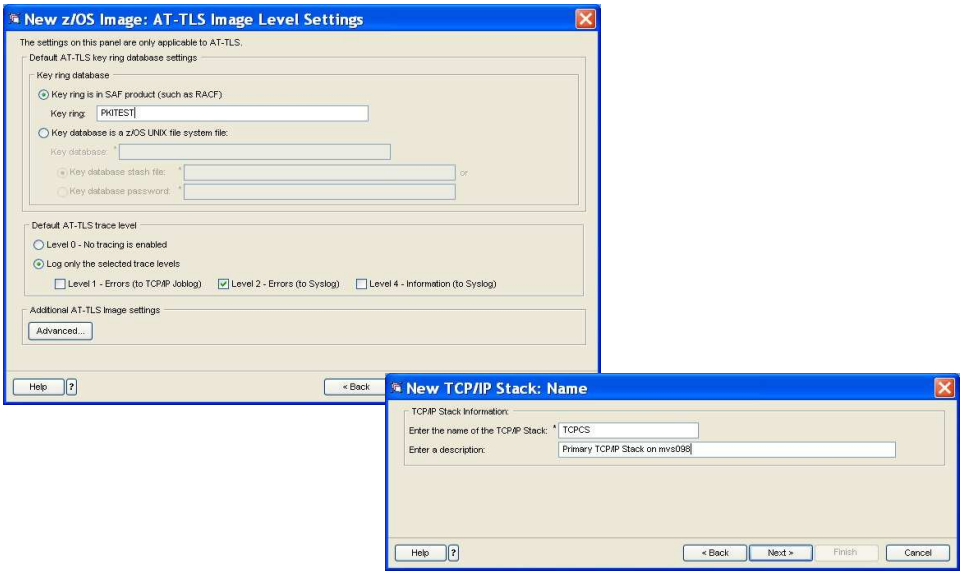
Use AT-TLS gold services for a TN3270 server



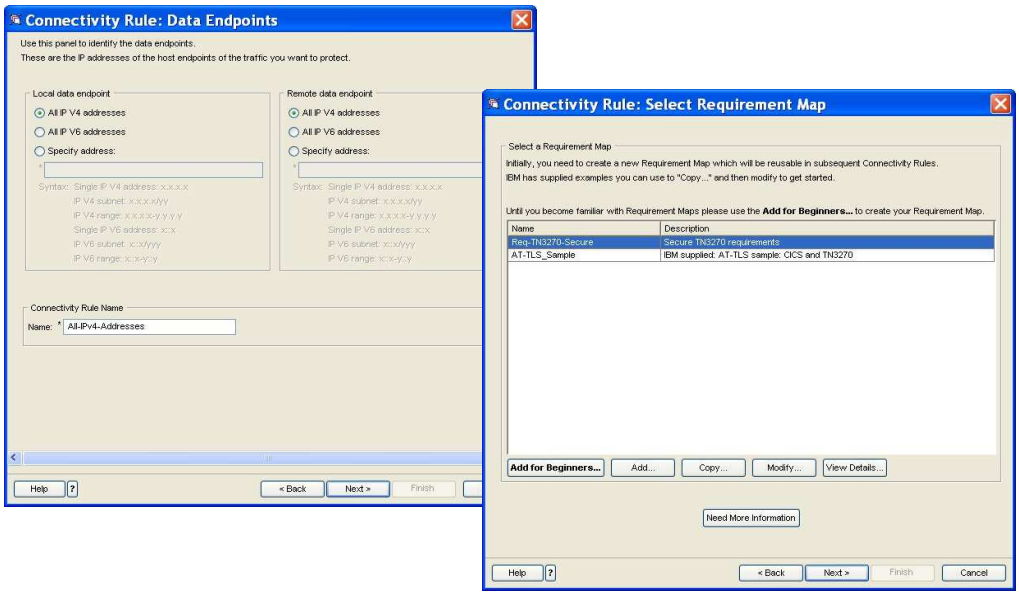
Specify which z/OS system these policies are intended for



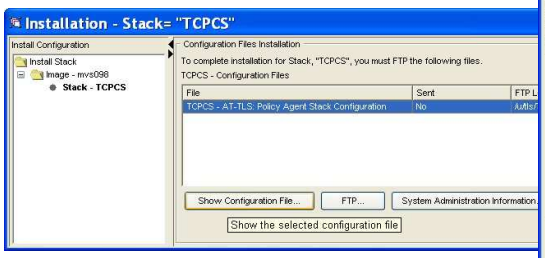
Specify system-wide defaults for AT-TLS - and add stack information

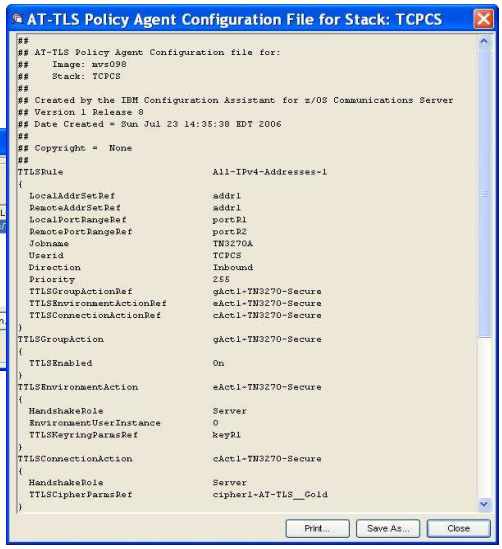


Identify the IP addresses (or ranges) that must use this requirement map

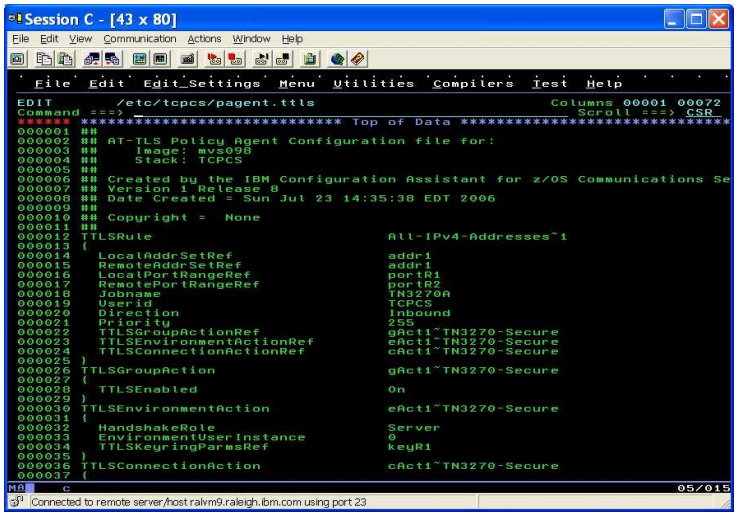


View and save (or FTP) the final AT-TLS policies





The generated AT-TLS policies in text format



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/tcpcs/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
TCPCS      READ
```

- **When TCP/IP starts with TCPCONFIG TTLS specified, it will issue the following message**
  - EZZ4248E TCPCS 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.

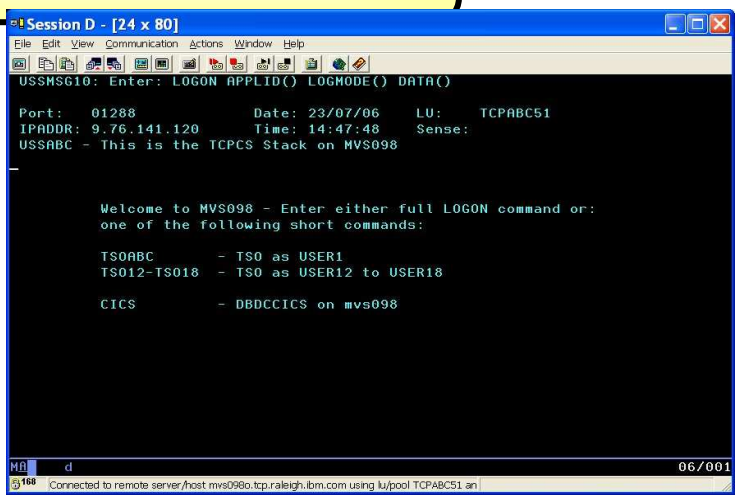
TN3270 server setup when using AT-TLS

```
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).



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

```
NETSTAT ALL TCP TCPCS ( CLI  TN3270A

Client Name: TN3270A                 Client Id: 000000DD
  Local Socket: ::ffff:9.42.105.45..2031
  Foreign Socket: ::ffff:9.76.141.120..1288
    BytesIn:            0000000000000000032
    BytesOut:           0000000000000000631
    SegmentsIn:         0000000000000000015
    SegmentsOut:        0000000000000000015
    Last Touched:       18:47:49          State:               Establsh
    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 00000DD 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
    CtraceClearText:          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.