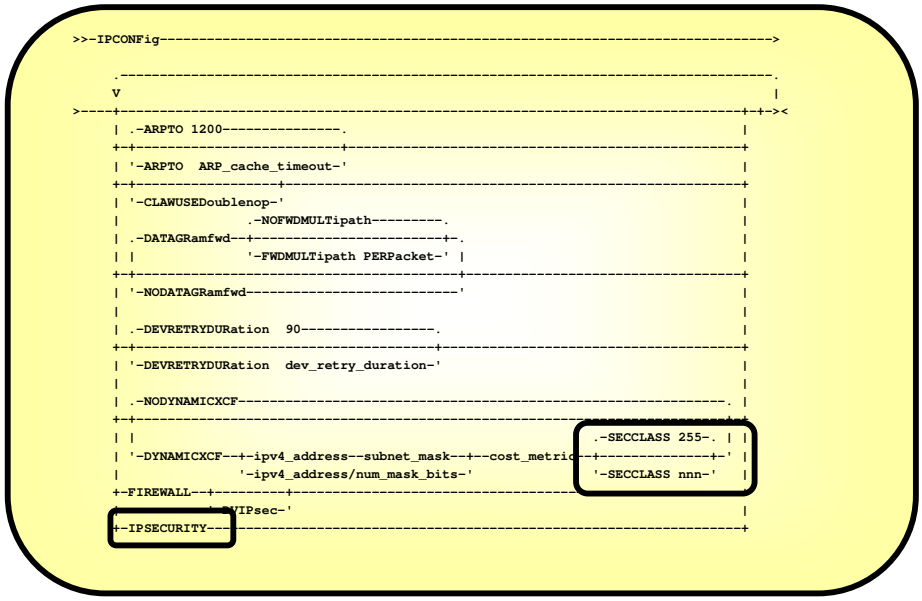
CS z/OS Integrated IP Security Configuration and Performance Data

Integrated IP security agenda

- **Configuring and enabling integrated IP Security**
- **Preliminary performance data**

Configuring and enabling integrated IP security

IPCONFIG syntax

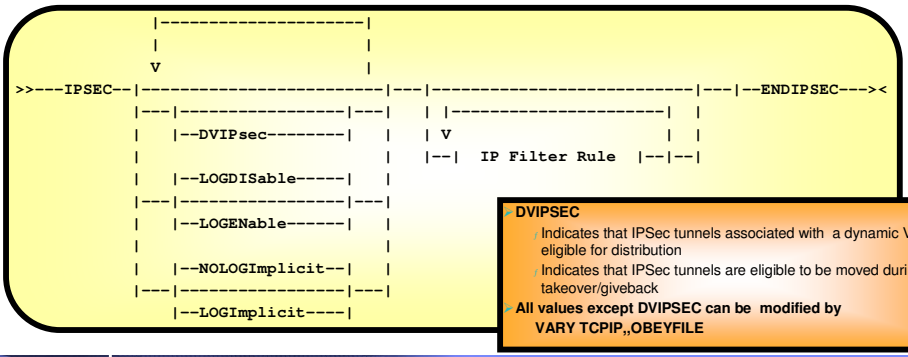


SECCLASS option on link definitions

- **Updated to include SECCLASS**
  - Used to uniquely identify an interface or group of interfaces with similar security requirements
  - Used as an IP filtering criteria
    - Can only be specified on rules with an action of permit/deny
    - Allows broad rules to be written for all IP traffic that uses a group of interfaces without explicit knowledge of IP address
  - Can be specified for all link types except VIRTUAL
  - To modify
    - Stop the device
    - Delete the LINK statement
    - Add the LINK statement with the updated value
    - Restart the device
  - Sample syntax:

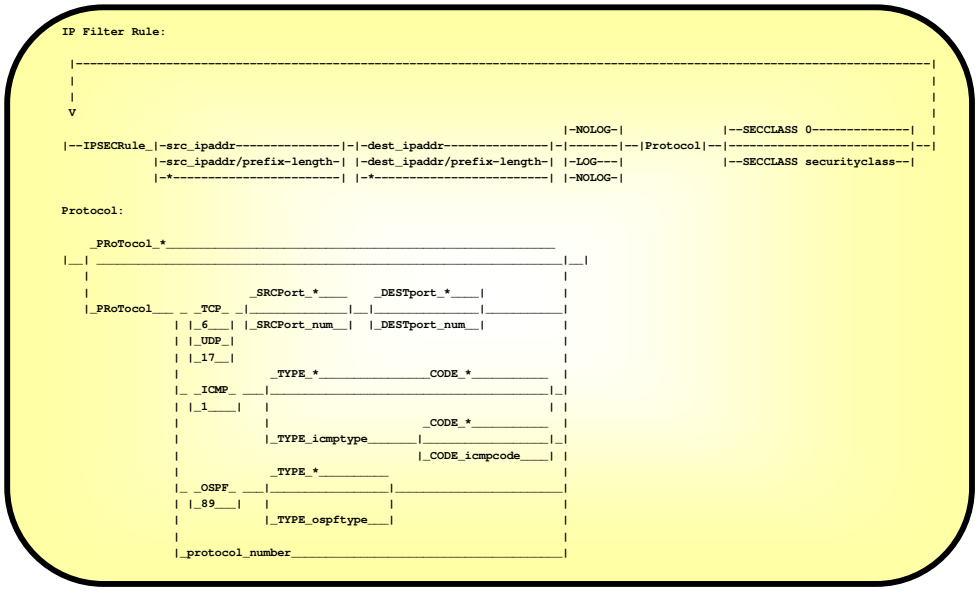
New IPSEC keyword in the TCP/IP profile

- **Allows you to define default IP filter rules**
  - User-defined rules are always "permit" rules and cannot include routed traffic
  - Default rules are in effect when
    - IPSec policy rules are not available
    - Specifically enabled by the ipsec command
  - Default rules are prepended to the "implicit" filter rules (which deny all traffic)
  - Controls filter logging options when default IP filter rules are in effect
- **Also controls the logging option for the implicit deny rules when default IP filter policy is active**
- **Requires IPSECURITY to be specified on the IPCONFIG statement**



- **DVIPSEC**
  - Indicates that IPSec tunnels associated with a dynamic VIPA are eligible for distribution
  - Indicates that IPSec tunnels are eligible to be moved during VIPA takeover/giveback
- **All values except DVIPSEC can be modified by VARY TCPIP,,OBEYFILE**

IPSec default filter rule specifications in the TCP/IP profile



IPSEC default filter rule specification example

```
IPSEC LOGENable
; Rule      SrcAddr DstAddr   Logging Protocol   SrcPort    DestPort     Secclass

; OSPF protocol used by Omproute
  IPSECRule *       *         NOLOG   PROTO OSPF

; IGMP protocol used by Omproute
  IPSECRule *       *         NOLOG   PROTO 2

; DNS queries to UDP port 53
  IPSECRule *       *         NOLOG   PROTO UDP  SRCPort *  DESTport 53

; Administrative access
  IPSECRule *       9.1.1.1   LOG     PROTO *                           SECCLASS 100
ENDIPSEC
```

- **Remember that these statements create bidirectional filters.**
- **The administrative access rule allows**
  - Traffic from remote IP address 9.1.1.1, any protocol over interfaces with a class of 100
  - Traffic to remote IP address 9.1.1.1, any protocol over interfaces with a class of 100

Policy Agent (Pagent) configuration files

- **Main configuration file**
  - New CommonIPSecConfig statement
    - Identifies an IPSec configuration file containing policy definitions that are common to all stacks in a z/OS image
- **Image configuration file**
  - New IPSecConfig statement
    - Identifies an IPSec configuration file containing policy definitions that are specific to a stack
- **IPSec configuration file (New)**
    - IpFilterPolicy
    - KeyExchangePolicy
    - LocalDynVpnPolicy
  - Stack-specific IPSec configuration file can be generated by the z/OS IP Security Configuration Assistant GUI or it can be edited by hand using a text editor, such as ISPF/PDF.
- **For additional details see**
  - "Chapter 15. Policy-based networking" in the "IP Configuration Guide"
  - "Chapter 18. IP Security" in the "IP Configuration Guide"
  - "Chapter 21. Policy Agent and policy applications" in the "IP Configuration Reference"

pcsearch command changes and a new ipsec command

- **Pasearch command additions**
  - New -v option
    - Displays IPSec policies
      - All IPSec policy entries (pasearch -v a)
      - IpFilter policy entries (pasearch -v f)
      - KeyExchange policy entries (pasearch -v k)
      - LocalDynVpn policy entries (pasearch -v l)
    - Can be used with other options to control output (e.g. pasearch -v a -n will just display the names of IPSec policy objects)

- **New ipsec command**
  - Displays IP security information
    - Current filter rules
    - Manual and dynamic IPSec tunnels
    - IKE tunnels
    - Stack interface information
    - Matching filter rules for a traffic pattern
  - Modifies IP security state
    - Change the filter policy the stack considers to be active
      - Default filter rules
      - IP Security filter rules
    - Activate/deactivate/refresh manual and dynamic IPSec tunnels
    - Deactivate/refresh IKE tunnels
  - Runs APF authorized
  - RACF profiles must be defined to use the ipsec command

ipsec command

Primary Command	Main functions provided
ipsec -f	•Display information about active filter set •Display information about default IP filter rules •Display information about IP Security filter rules •Make the default IP filter rules the active filter set •Make the IP Security filter rules the active filter set
ipsec -m	•Display information about manual tunnels •Activate manual tunnels •Deactivate manual tunnels
ipsec -k	•Display information about IKE tunnels •Deactivate IKE tunnels •Refresh IKE tunnels
ipsec -y	•Display information about dynamic tunnels (stack's view) •Display information about dynamic tunnels (IKED's view) •Activate dynamic tunnels •Deactivate dynamic tunnels •Refresh dynamic tunnels
ipsec -i	•Display interface information
ipsec -t	•Locate matching filter rule
ipsec -o	•Display NATT port translation table information
ipsec -?	Help

See the "IP System Administrator's Commands" for the complete syntax

ipsec command protection via SERVAUTH profiles

- Command access controlled by profiles in the SERVAUTH class

Resource name	ipsec options allowed
EZB.IPSECCMD.sysname.tcpprocname.*	All of ipsec options
EZB.IPSECCMD.sysname.tcpprocname.DISPLAY	-f display -m display -k display -y display -t -i -o
EZB.IPSECCMD.sysname.tcpprocname.CONTROL	-f default -f reload -m activate -m deactivate -k deactivate -k refresh -y activate -y deactivate -y refresh

Sample JCL job to define these profiles provided in SEZAINST(EZARACF)

IKE daemon

- **Provides for the negotiation of IPSec SAs using the Internet Key Exchange (IKE) as defined in RFC 2409, including support of RFC 3947 (Negotiation of NAT-Traversal in the IKE)**

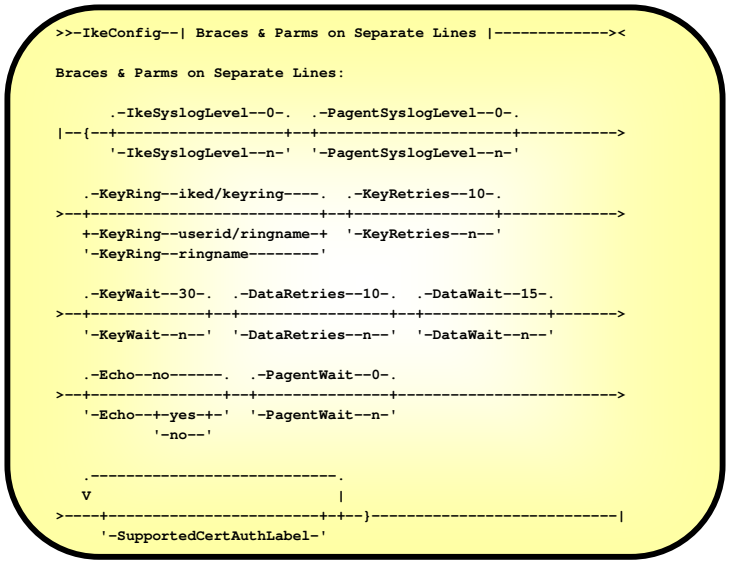
- **APF authorized UNIX application**
  - Can be started from UNIX shell (iked) or started proc (sample in SEZAINST(IKED))

- **IKED_FILE**
  - Specifies where to find the IKE Daemon configuration file
    - IKED_FILE=/etc/security/iked.conf
  - If not specified the default is /etc/security/iked.conf

- **IKED_CTRACE_MEMBER**
  - Specifies the name of a parmlib member in the form CTIIKExx that contains default CTRACE settings
    - Example: IKED_CTRACE_MEMBER=CTIIKE3A
  - If not specified the default is CTIIKE00
  - Must be set prior to starting IKED
    - CTRACE settings only read during IKED initialization

IKE daemon - IkeConfig statement syntax

NOTES



IKE daemon configuration file

NOTES

- Contains an IkeConfig statement
  - Enables additional syslog messages
  - Controls the retransmission of IKE messages
  - Defines the location of a keyring containing IKED's certificates
  - Allows syslog messages to be echoed to the job log
  - Controls how long IKE should wait when connecting to Pagent
  - Identifies the labels of supported certificate authorities (CAs)
    - Used to inform a remote security endpoint of acceptable CAs
- Sample provided in /usr/lpp/tcpip/samples/iked.conf
- Search order
  - The name of an HFS file or MVS file specified by the IKED_FILE environment variable
  - /etc/security/iked.conf
- Generated by the z/OS IP Security Configuration Assistant GUI
- Display the contents of the IKE Daemon configuration file

```
--+-MODIFY-+--procname,DISPLAY--------------------------------
  '-F------'
```

Process the specified IKE Daemon configuration file

- The following parameters cannot be modified
  - KeyRing
  - PagentWait

```
--+-MODIFY-+--procname,REFRESH--+--------------------+---------|
  '-F------'                    +-,FILE='filename'---+
                               '-,FILE=//'filename'-'
```

Enabling integrated IP security for a stack

- **Ensure Pagent is configured and started**
  - Define IPSec policy
  - Update Pagent configuration file to contain IPSecConfig and optionally CommonIPSecConfig
- **Ensure TRMD is configured and started**
- **Ensure syslogd is configured and started**
  - TRMD will write IPSec messages to local4
- **Update TCP/IP profile**
  - Add IPSECURITY to IPCONFIG statement
  - Classify devices by adding SECCLASS (optional)
  - Define default filter rules
- **Create security definitions for ipsec command**
  - Details provided in the Integrated IPSec Externals section
    - Update the SERVAUTH class
    - Restrict access to the marker files
- **Authorize the stack to ICSF**
  - If hardware encryption is available

Authorize the stack to ICSF

NOTES

- Cryptographic coprocessor service
  - Services used by IPSec when using a cryptographic coprocessor
    - CSFCKI
    - CSFDEC1
    - CSFENC1
    - CSFRNG
    - CSFCKM
      - If triple DES hardware cryptographic support is available
    - CSFOWH1
  - Access to the stack must be granted to CSFSERV (if controlled by RACF)
    - Define profiles in the CSFSERV class (if not defined)
      - RDEFINE CSFSERV service-name UACC(NONE)
    - Give stack access
      - PERMIT service-name CLASS(CSFSERV) ID(stackname) ACCESS(READ)
    - For applications that run under a specific user's ID, such as oping, give the user's ID access to the profiles:
      - PERMIT service-name CLASS(CSFSERV) ID (userid)
    - Activate (if necessary) the CSFSERV class and refresh the in-storage RACF profiles
      - SETROPTS CLASSACT(CSFSERV)
      - SETROPTS RACLIST(CSFSERV) REFRESH
    - Ensure the MAXLEN ICSF/MVS installation option is set to 65535 or greater
- CP assist for cryptographic functions
  - Services used by IPSec when using the CP assist functions
    - CSNBSYE1
    - CSNBSYD1
  - The CP Assist functions are not RACF controlled

Enabling the IKE daemon

- **Create the IKE daemon configuration file**
  - Sample in /usr/lpp/tcpip/samples/iked.conf
- **If starting from the UNIX shell**
  - set _BPX_JOBNAME (optional)
- **If starting from a cataloged procedure**
  - Update sample from SEZAINST(IKED)
- **Update the PORT statement in the TCP/IP profile to reserve UDP ports 500 and 4500**
- **Authorize the IKE daemon to the External Security Manager (ESM)**
- **Ensure syslogd is configured and started**
  - The IKE daemon will write syslog records to local4
  - For performance reasons it is recommended that IKE daemon syslog records be written to a zFS file

Enabling the IKE daemon (continued)

- **Define the location of the IKE daemon configuration file and parmlib member for CTRACE**
  - IKED_FILE and IKED_CTRACE_MEMBER
- **If RSA signature is being utilized, set up the IKE daemon keyring**
- **Performance considerations**
  - Set appropriate dispatching priority at or just below TCPIP's priority
  - If running WLM should be assigned to the SYSSTC service class
- **Decide how you want the IKE daemon to be started**
  - Automated
    - AUTOSTART in the TCP/IP profile (use this technique if there is only 1 IP security stack running)
    - Using the COMMNDxx member of parmlib
  - From UNIX shell
    - iked
  - From operator's console
    - S IKED

Authorize IKE daemon

NOTES

- Allow the IKE aaemon to access SYS1.PARMLIB as follows:
  - PERMIT SYS1.PARMLIB ID(IKED) ACCESS(READ)
- Add user ID IKED with UID of 0:
  - ADDUSER IKED DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
  - SETROPTS GENERIC(STARTED) REFRESH
- If starting the IKE daemon via a proc add IKED to the STARTED class as follows:
  - RDEFINE STARTED IKED.* STDATA(USER(IKED))
  - SETROPTS RACLIST(STARTED) REFRESH
- If using RSA Signature enable IKED to access certificates on an ESM keyring as follows:
  - Define DIGTCERT facility (if not already defined)
    - RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
    - RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
  - Give the IKE daemon access
    - PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IKED) ACCESS(READ)
    - PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(IKED) ACCESS(READ)
  - SETROPTS RACLIST(FACILITY) REFRESH

Setting up the IKE keyring

NOTES

- Set up the DIGTCERT facility (if not already defined)
  - RDEFINE FACILITY IRR.DIGTCERT.ADD UACC(NONE)
  - RDEFINE FACILITY IRR.DIGTCERT.ADDRING UACC(NONE)
  - RDEFINE FACILITY IRR.DIGTCERT.CONNECT UACC(NONE)
  - RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE)
  - RDEFINE FACILITY IRR.DIGTCERT.GENREQ UACC(NONE)
  - SETROPTS RACLIST(FACILITY) REFRESH
- Give DIGTCERT access to the userid that will own the IKE daemon's keyring
  - PERMIT IRR.DIGTCERT.ADD CLASS(FACILITY) ID(userid) ACC(CONTROL)
  - PERMIT IRR.DIGTCERT.ADDRING CLASS(FACILITY) ID(userid) ACC(UPDATE)
  - PERMIT IRR.DIGTCERT.CONNECT CLASS(FACILITY) ID(userid) ACC(CONTROL)
  - PERMIT IRR.DIGTCERT.GENCERT CLASS(FACILITY) ID(userid) ACC(CONTROL)
  - PERMIT IRR.DIGTCERT.GENREQ CLASS(FACILITY) ID(userid) ACC(CONTROL)
  - PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(userid) ACC(CONTROL)
  - PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACC(UPDATE)
- Create the IKE daemon keyring
  - RACDCERT ID(IKED) ADDRING(IKEYRING)
- Add CA certificates (as needed)
  - RACDCERT ID(IKED) ADD('USER1.EXTCA1.CERT') WITHLABEL('External CA') CERTAUTH
- Connect CA Certificates to the IKE daemon's keyring
  - RACDCERT ID(IKED) CONNECT(CERTAUTH LABEL('IBM Local Certificate Authority') RING(IKEYRING) USAGE(CERTAUTH))

Setting up the IKE keyring (continued)

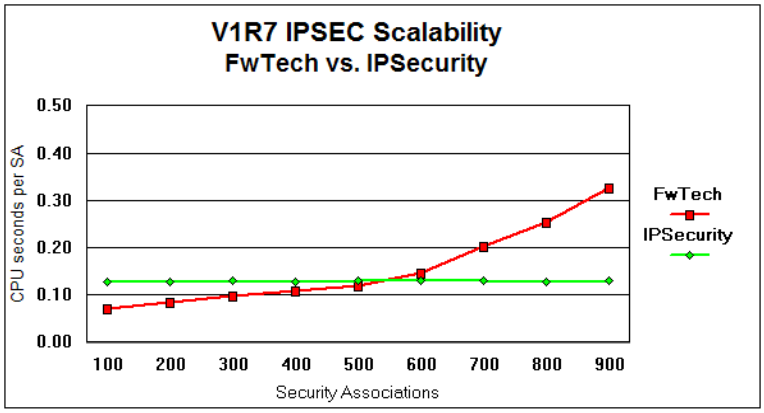
NOTES

- Obtain certificates
  - Example
    - Create a self-signed certificate
      - RACDCERT ID(IKED) GENCERT SUBJECTSDN(CN('IBM IKE Server') OU('Inventory') O('IBM') C('US')) WITHLABEL('IKE Server') ALTNAME(DOMAIN('ibm.com'))
    - Create a certificate request
      - RACDCERT ID(IKED) GENREQ(LABEL('IKED server')) DSN('USER1.IKED.GENREQ')
    - Send the certificate request to the certificate authority
      - Typically the B64 certificate request in USER1.IKED.GENREQ will be cut and pasted into a Web page
    - Receive the returned certificate into a data set (for example, USER1.IKED.CERT)
    - Replace the self-signed certificate with the certificate created by the certificate authority
      - RACDCERT ID(IKED) ADD('USER1.IKED.CERT') WITHLABEL('IKED server')
    - Connect the certificate to the IKE daemon's keyring
      - RACDCERT ID(IKED) CONNECT(LABEL('IKED server') RING(IKEYRING) USAGE(PERSONAL))
  - Additional notes
    - The certificate must contain your local security endpoint's ID in either
      - The SubjectName
        - If ID is x500.DN
      - The SubjectAltName
        - If ID is user@fqdn, fqdn, or IPv4 address
    - The certificate must be authorized for creating a digital signature
      - The digitalSignature bit must be on in the KeyUsage field

Preliminary performance data

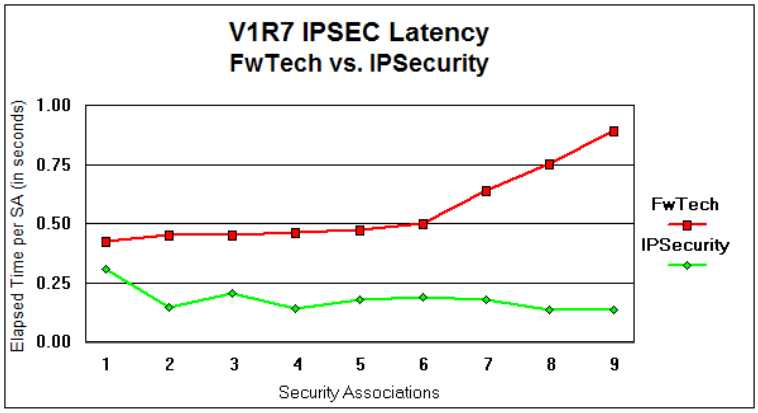
CPU cost of setting up an IPSec security associations

- **IPSec scalability**
  - CPU cost per SA is the same as one adds more Security Associations



Time to set up an IPSec security association

- **IPSEC latency**
  - Elapsed time it takes for an SA to be established for a connection is approximately the same as one adds more SA's



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	CICS	IMS	MQSeries	Tivoli
IBM(logo)	Cloudscape	Informix	OS/390	WebSphere
e(logo)business	DB2	iSeries	OS/400	xSeries
AIX	DB2 Universal Database	Lotus	pSeries	zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

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 and/or changes in the product(s) and/or program(s) 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 (e.g., 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.

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.