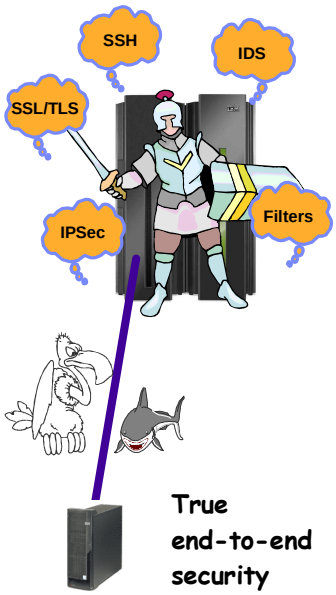
This presentation describes the enhancements to z/OS V1R11 Communications Server for security.

Security

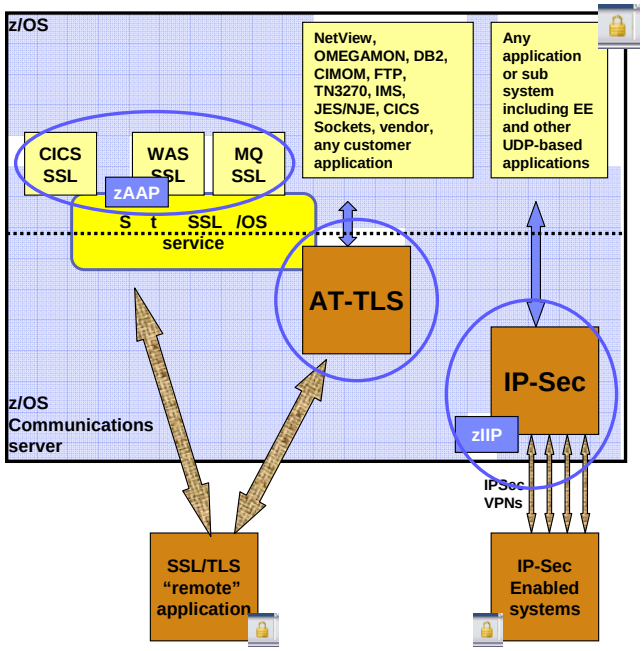
- IPSec enhancements
- AT-TLS enhancements



There are two main groups of enhancements to the z/OS Communications Server networking security functions in this release. The AT-TLS function is enhanced with support for many new SSL features. IPSec is enhanced within the network management area.

z/OS network encryption overview

- Two general types of network encryption:
  - VPNs are Virtual Private Networks
    - System to system
    - Transparent to applications
  - SSL is Secure Sockets Layer
    - Application to application
    - SSL is also known as TLS, Transport Layer Security
    - SSL services are provided by the System SSL z/OS component



This slide is a brief review of the network security technologies that are supported on z/OS.

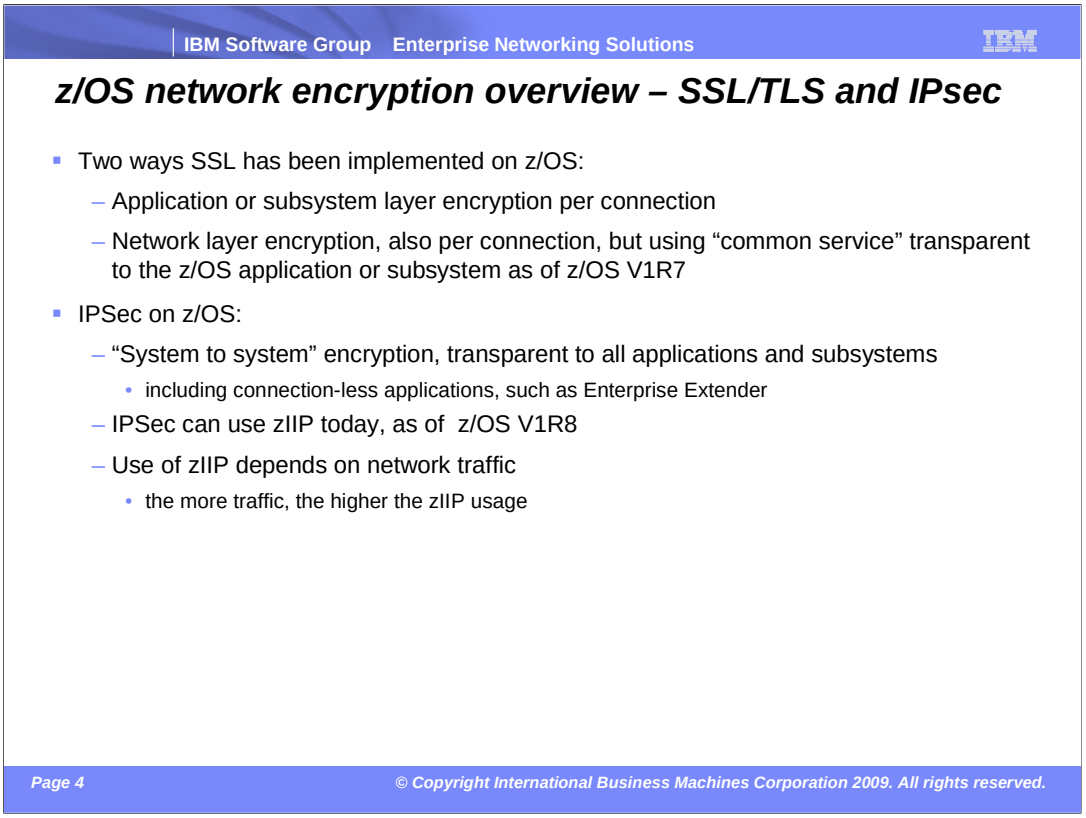
Network security generally offers four basic services for securing network communication with partner systems and applications.

The first network security service is end point authentication during secure channel setup, making sure the partner is who it claims to be. The end point can be a user, an application, or an IP node. In SSL/TLS, end point authentication is part of the SSL/TLS handshake. In IPSec, end point authentication is part of the dynamic VPN setup done by IKE. The next slide describes the SSL and IPsec parts of the diagram on this slide.

The second network security service is data confidentiality, making sure only the intended receiver can understand the data content.

The third network security service is message authentication, making sure each message comes from the intended and authenticated partner.

The fourth network security service is message integrity, making sure that data was not changed somewhere in the network since it was sent by the authenticated partner.



SSL/TLS works per TCP connection. SSL/TLS is not supported for transport protocols other than TCP. Therefore, there is no support for UDP, hence no SSL/TLS support for traffic such as Enterprise Extender. On z/OS, SSL/TLS services are based on the z/OS System SSL components with which applications interface directly (by calls to system SSL) or indirectly (by way of AT-TLS).

SSL/TLS can be implemented by way of application calls directly into the System SSL component of z/OS. Such APIs are supported for C/C++ and Java™ only.

SSL/TLS can also be implemented in a way that does not require any application or subsystem change by way of Application Transparent SSL/TLS support in the Communications Server.

IPSec works for all IP traffic between two IP hosts including UDP traffic. This is the reason why IPSec is the recommend network security technology to secure Enterprise Extender traffic.

IPSec enhancements

- In compliance with RFC 2408, in V1R11 z/OS Communications Server IKED supports an exponential back-off retransmission algorithm
  - This is a more efficient retransmission algorithm, which will also help improve IKED's response to network congestion situations
- In V1R11, z/OS Communications Server reports additional tunnel selector and attribute information on
    - the ipsec command
    - network management interfaces (NMIs)
    - SMF records
  - This information can currently be inferred from other attributes, but is provided for completeness
- z/OS V1R11 continues to support the IKE version 1 protocol, but has issued a statement of direction for support of IKE version 2

z/OS V1R11 modifies a few selected aspects of the IKEv1 protocol implementation to better match the way other platforms have implemented this function.

The changed options have an impact on the ipsec command output and NMI interface.

The new IkeRetries parameter controls the number of times that any IKE message is retransmitted. The default value is six times. This replaces the KeyRetries and DataRetries parameters, which are now ignored.

The new IkeInitWait parameter controls the number of seconds that IKE waits before retransmitting a message the first time. The default value is two seconds. This replaces the KeyWait and DataWait parameters, which are now ignored.

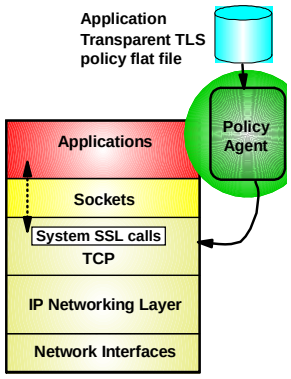
Subsequent retransmissions will double the delay of the previous retransmission. So using the default IkeInitWait of two seconds, the second retransmission will occur four seconds after the first; the third retransmission will occur eight seconds after the second, and so forth. Using the default values of IkeRetries and IkeInitWait, IKE retransmissions for any given message will time out after four minutes, 14 seconds.

IBM has issued a statement of direction that z/OS Communications Server will add support for the newest IKE protocol version, IKEv2, in a future release. Some of the IPSec enhancements you see in z/OS V1R11 are in preparation for support of IKEv2. There are rather significant infrastructure changes in support of IKEv1 included in z/OS V1R11, laying the foundation for adding IKEv2 support in a future release.

Here is the statement of direction. ***IBM intends to update z/OS with support for the latest Internet Key Exchange protocol, version 2 (IKEv2), as defined by industry standards documented in "Internet Key Exchange (IKEv2) Protocol", RFC4306 and "IKEv2 Clarifications and Implementation Guidelines", RFC4718 and other publications. This support is intended to allow z/OS to maintain compliance with industry standard IPv6 profiles, and to expand the options available to network administrators for configuring IPSec-protected communications with z/OS systems.***

AT-TLS enhancements

- AT-TLS to support new System SSL functions that have been added to System SSL since z/OS V1R7:
  - TLS V1.1
  - Using RFC3280 to validate a certificate
  - Negotiation and use of a truncated HMAC
  - Negotiation and use of a maximum SSL fragment size
  - Negotiation and use of handshake server name indication
  - Setting the CRL LDAP server access security level
- AT-TLS is also updated to address FIPS 140-2 requirements for applications that use AT-TLS to provide secure connections.
- AT-TLS performance enhancements for short-lived connections



AT-TLS was initially developed and implemented in z/OS V1R7. Since then, System SSL has added support for new features and protocol extensions. In z/OS V1R11, the AT-TLS support is enhanced to allow those features to be configured using the Configuration Assistant and for AT-TLS to exploit these new features.

AT-TLS now supports an updated TLS protocol – the TLS version 1.1 protocol level.

In combination with System SSL, AT-TLS is also enhanced to aid in addressing FIPS 140-2 requirements, allowing the system SSL capabilities to be configured and used.

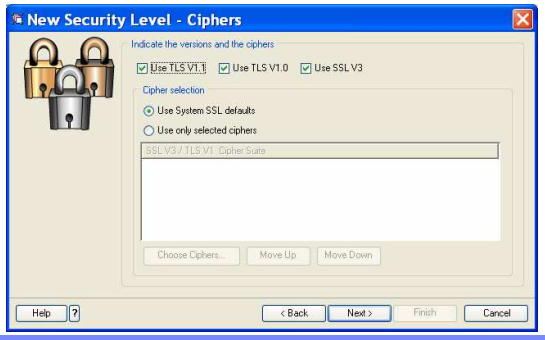
RFC 4366 defines extensions to the TLS protocol to add functionality. Most of the extensions were created to help clients on wireless networks or other bandwidth or memory restricted environments. The extensions are compatible with earlier versions, meaning TLS implementations which do not support these extensions will ignore them. The extensions are only supported when TLSv1.0 or TLSv1.1 are negotiated as the security level. A client or server has the option to require an extension be accepted by the remote partner. The connection can be failed if the extension is not supported. This concept is configured using a Required/Optional/Off syntax with AT-TLS. Required indicates the remote partner must support the TLS extension or the TLS handshake fails. Optional indicates the connection is allowed if the remote partner doesn't support the extension. Off indicates the extension is not supported.

TLS Version 1.1 support by AT-TLS

- Compared to the TLS 1.0 protocol, the TLS 1.1 protocol contains some security improvements, clarifications, and editorial improvements. The major changes are:
  - The implicit Initialization Vector (IV) is replaced with an explicit IV to protect against CBC attacks
  - Handling of padding errors is changed to use the bad_record_mac alert rather than the decryption_failed alert
    - This will protect against cipher block chaining (CBC) attacks
  - IANA registries are defined for protocol parameters
  - Premature closes no longer cause a session to be non-resumable
  - Additional informational notes were added for various new attacks on TLS

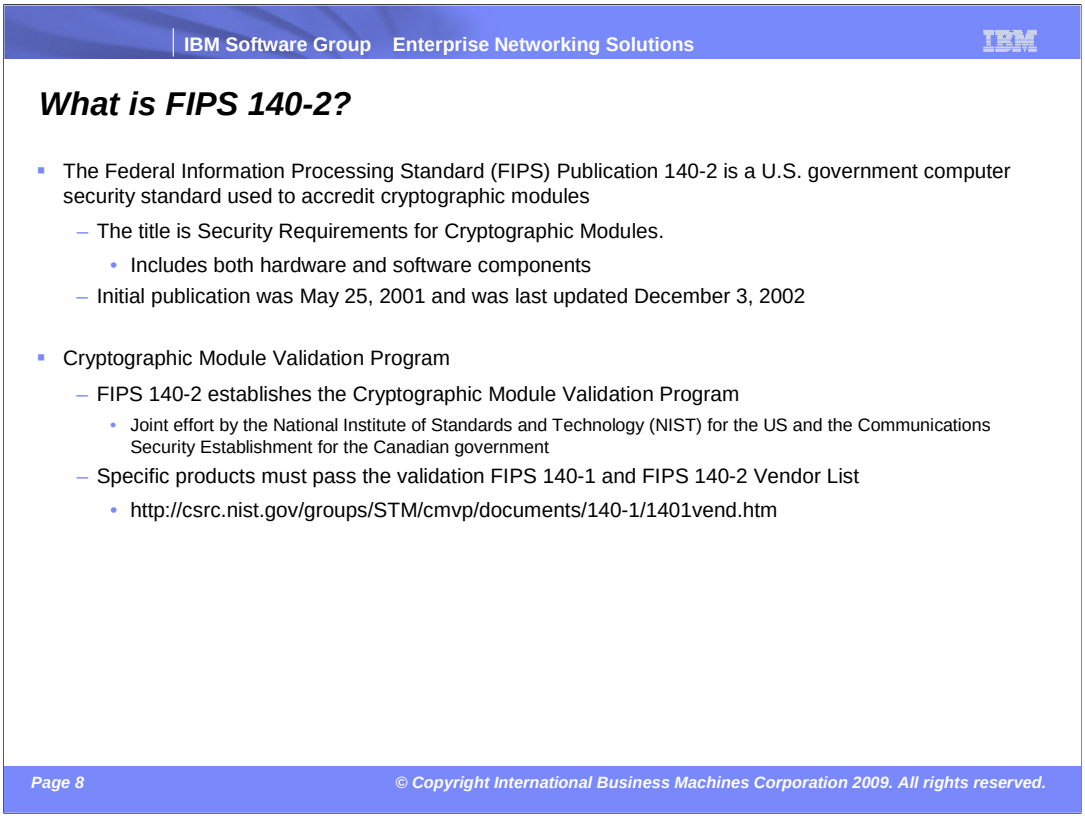
"*The Transport Layer Security (TLS) Protocol Version 1.1*", RFC 4346

Perspective -> AT-TLS -> Security Levels -> Add -> Next



System SSL adds support for the TLS Version 1.1 protocol in z/OS V1R11. AT-TLS also added that support in z/OS V1R11.

TLSv1.1 can be configured by using the check box for the TLSv1.1 on the New Security Level – Ciphers panel.



FIPS 140-2 defines four levels of security, named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

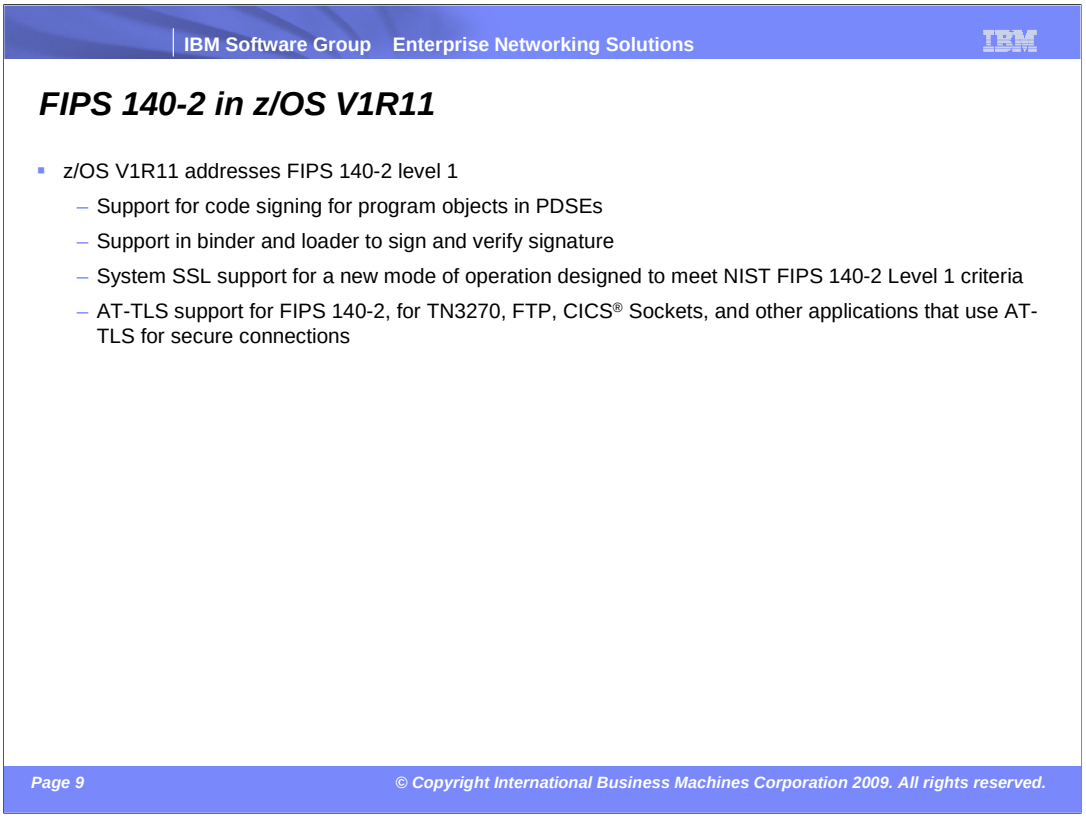
Security level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (for example, at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a security level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a security level 1 cryptographic module is a personal computer (PC) encryption board.

Security level 2 improves upon the physical security mechanisms of a security level 1 cryptographic module by requiring features that show evidence of tampering. This includes tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. This level also requires pick-resistant locks on covers or doors to protect against unauthorized physical access.

In addition to the tamper-evident physical security mechanisms required at security level 2, security level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at security level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms can include the use of strong enclosures and tamper detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Security level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroing of all plaintext CSPs.

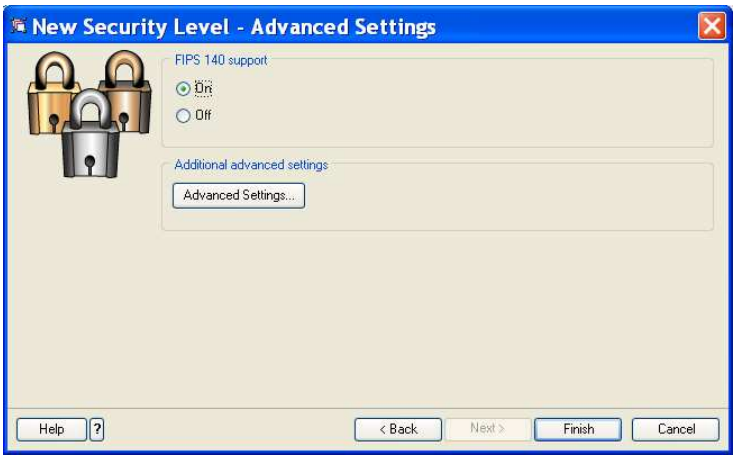


z/OS V1R11 addresses FIPS 140-2 level 1. It provides support for code signing for program objects in PDSEs. It provides support in the binder and loader to sign and verify signatures. System SSL support for a new mode of operation is designed to meet NIST FIPS 140-2 Level 1 criteria. AT-TLS adds support for FIPS 140-2 for TN3270, FTP, CICS Sockets, and other applications that use AT-TLS for secure connections.

AT-TLS support for System SSL FIPS 140-2 mode

- A new advanced settings attribute in an AT-TLS security level

Perspective -> AT-TLS -> Security Levels -> Add -> Next -> Next



The Advanced Settings have a radio button to configure FIPS 140-2 support as either On or Off. Off is the default. That is all you have to configure – the rest is taken care of by the AT-TLS and System SSL components.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

CICS z/OS

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

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

Other company, product, or 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 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.

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.

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.