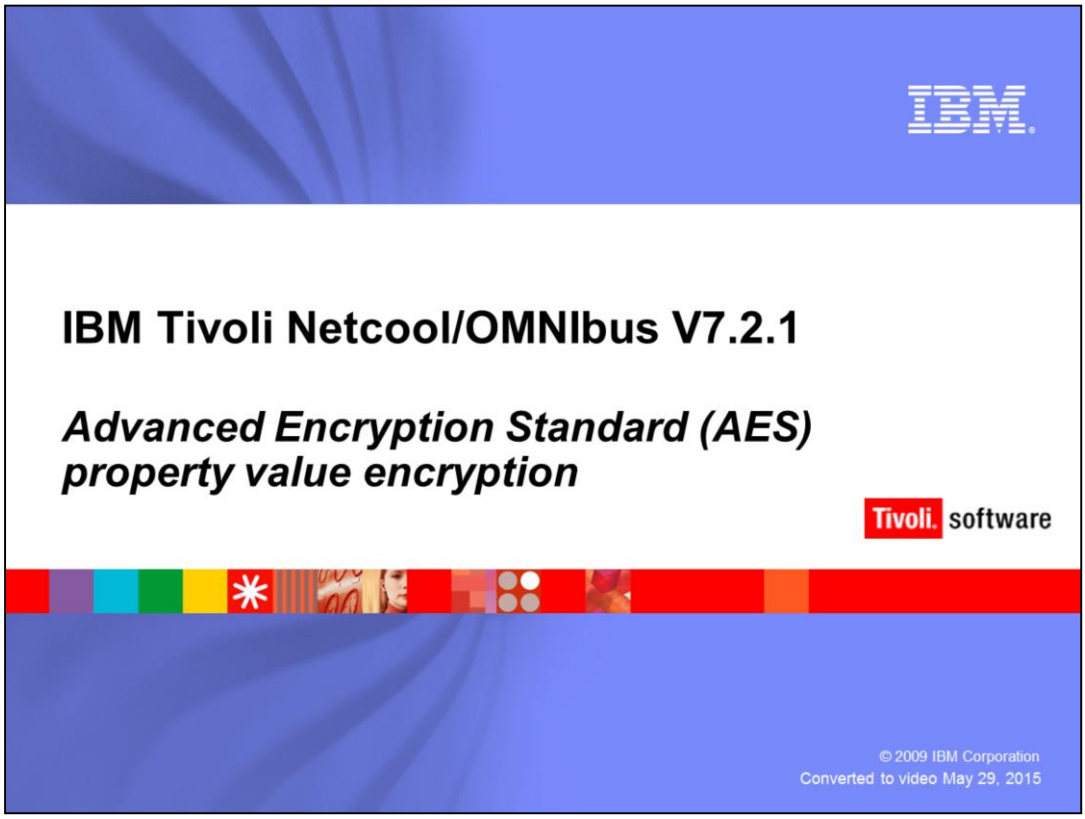
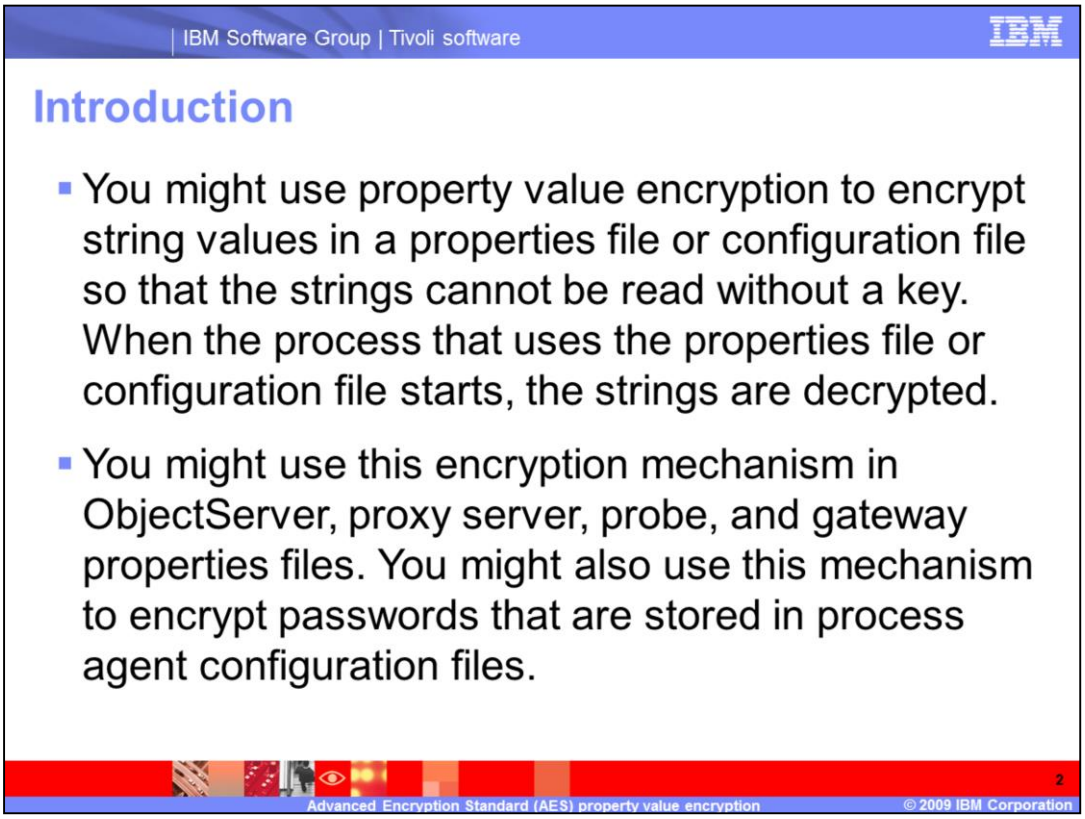
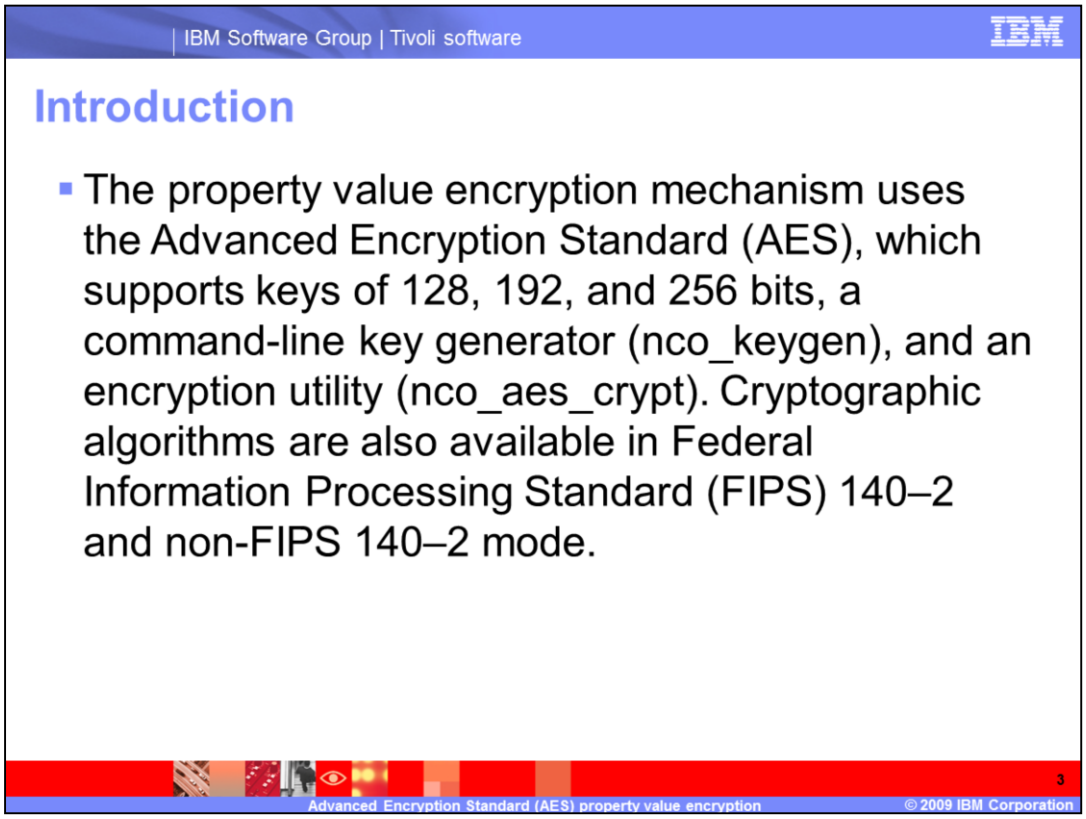


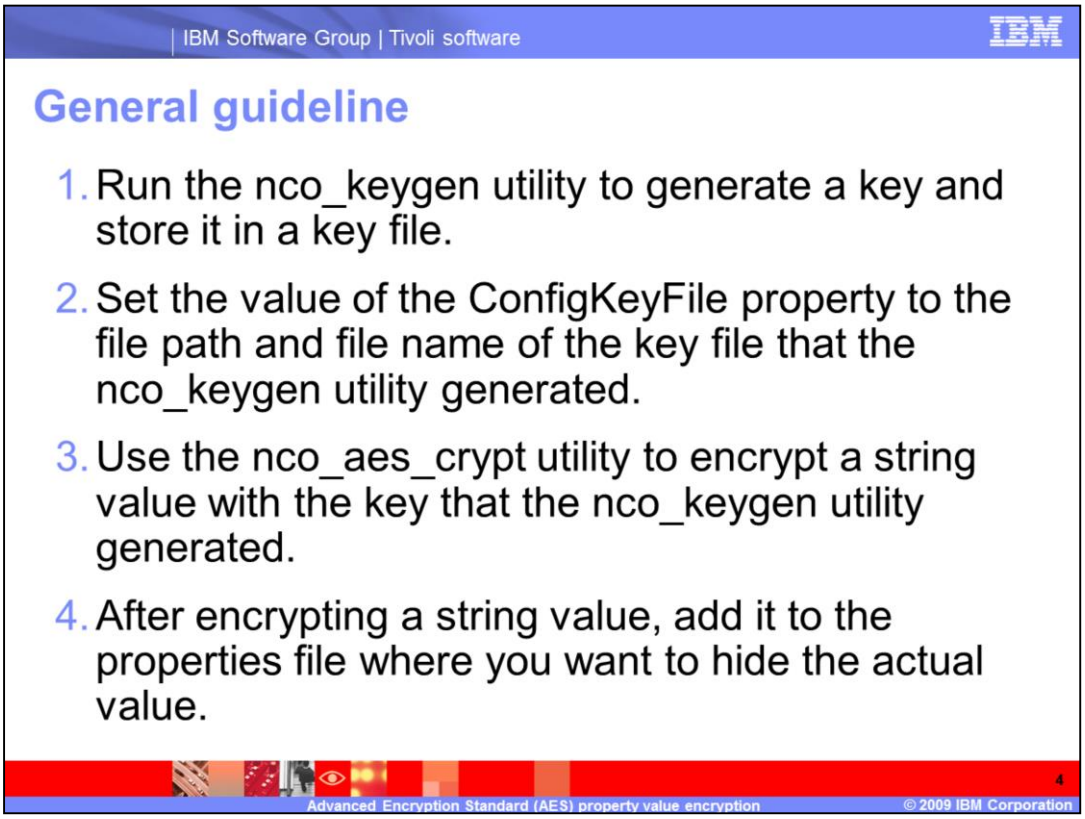
Hello, and welcome to the OMNIbus IBM Education assistance module, AES property value encryption.



You might use property value encryption to encrypt string values in property or configuration files so that the strings cannot be read without a key. When a process uses the property or configuration file starts, the strings are decrypted. You might use this encryption in ObjectServer, proxy server, probe, and gateway properties files. You might also use this encryption for passwords that are stored in process agent configuration files.



OMNIbus 7.2.1 might use the AES standard. The AES standard, in OMNIbus, provides greater key support, the nco_keygen key generator, and the nco_aes_crypt utility. Cryptographic algorithms are also available in Federal Information Processing Standard (FIPS) and non-FIPS mode.



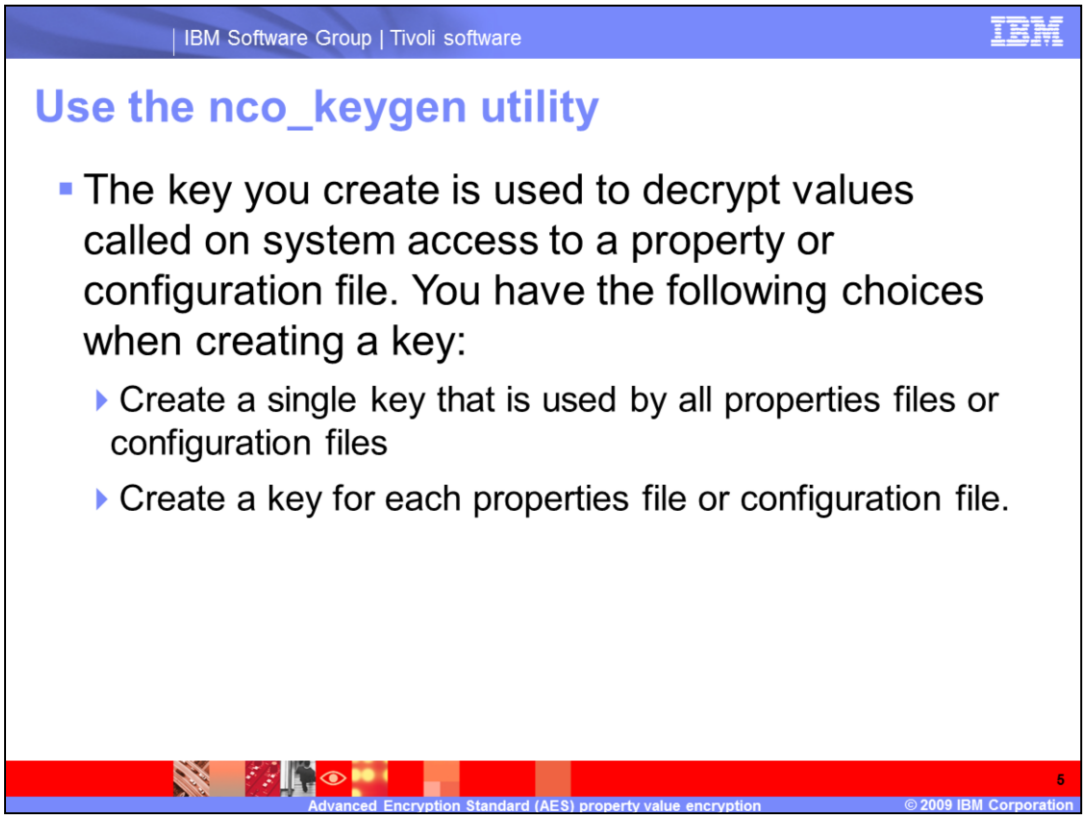
The general guideline to use the new AES encryption standard are to:

1.Run the nco_keygen utility to generate a key and store it in a key file.

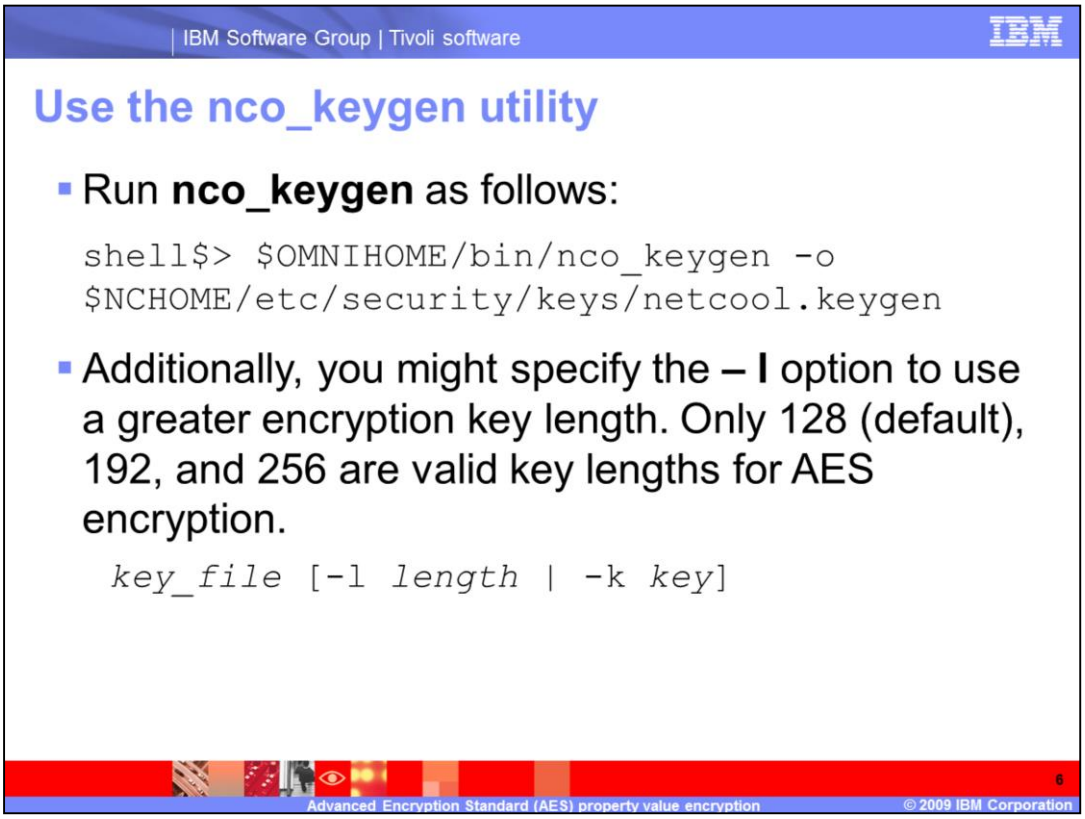
2.Set the value of the ConfigKeyFile property to the file path and file name of the key file that the nco_keygen utility generated.

3.Use the nco_aes_crypt utility to encrypt a string value with the key that the nco_keygen utility generated.

4.After encrypting a string value, add it to the properties file within which you want to hide the actual value.



You might create a single key that is used by all the properties or configuration files, or create a key for each properties or configuration file.

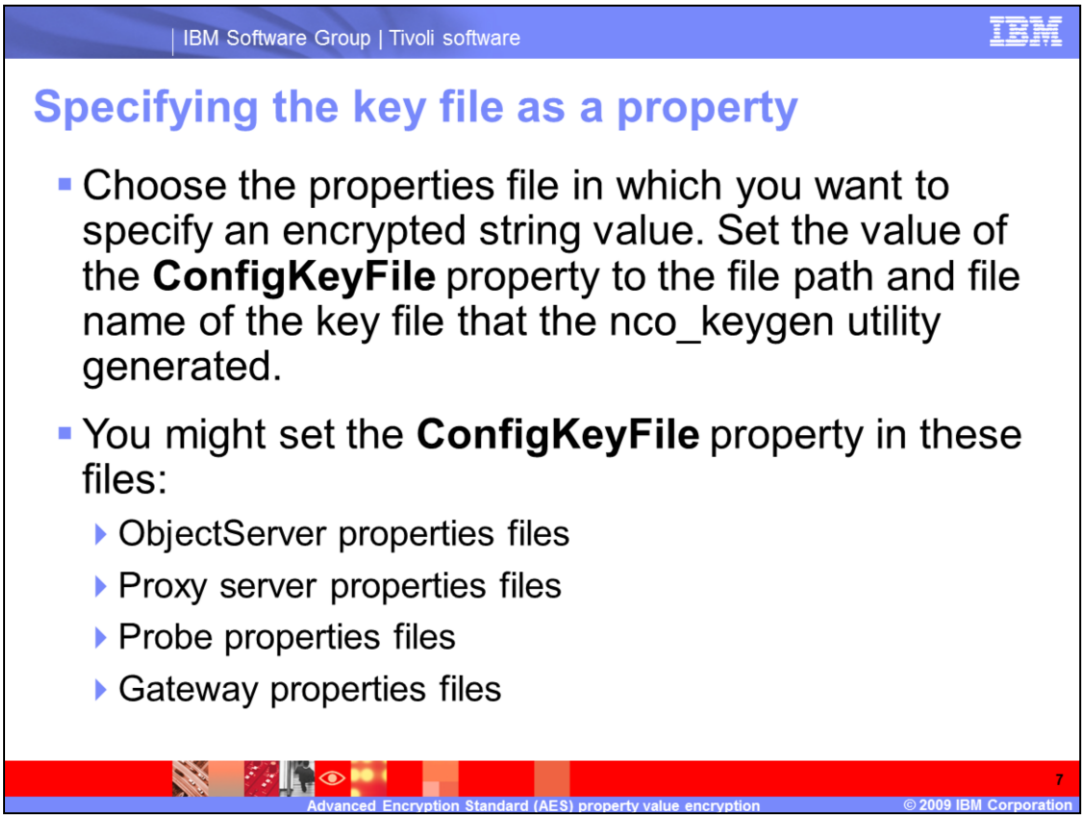


The nco_keygen command might be run with the default values or additional parameters. Additional parameters include:

key_file which represents the output file path and file name to which the key is saved.

length 3which represents the length in bits of the key, as specified by you. This number must be divisible by 8 to make a whole number of bytes. The default is 128. Only 128, 192, and 256 are valid key lengths for AES encryption.

And key which represents the value of your specified key in hexadecimal digits.



Choose the properties file in which you want to specify an encrypted string value. Set the value of the **ConfigKeyFile** property to the file path and file name of the key file that the nco_keygen utility generated.

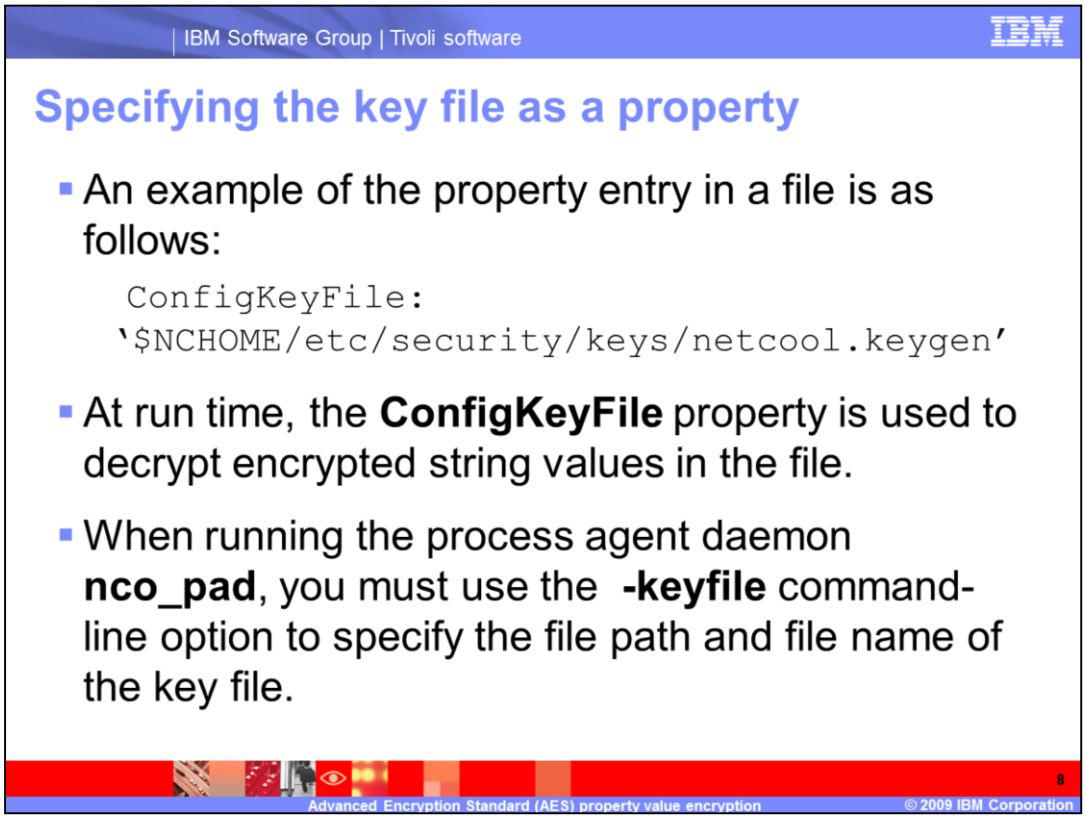
You might set the **ConfigKeyFile** property in these files:

ObjectServer properties files

Proxy server properties files

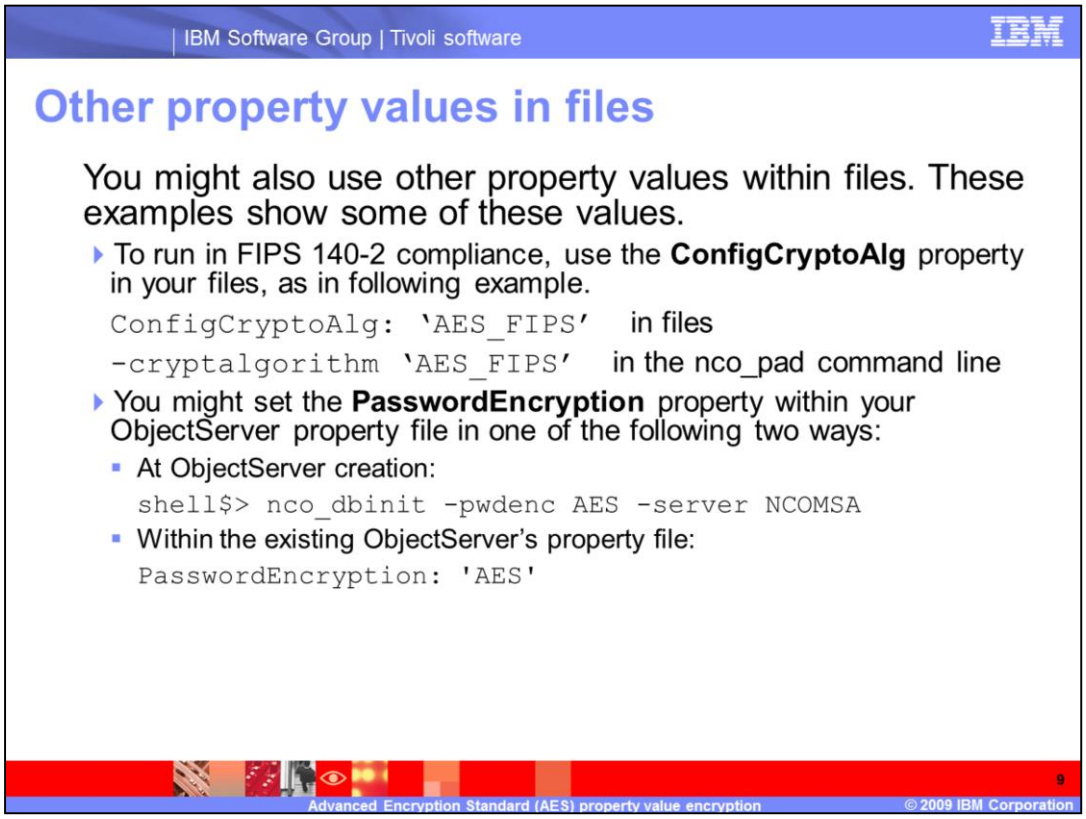
Probe properties files

Gateway properties files.



At run time, the **ConfigKeyFile** property is used to decrypt encrypted string values in the file.

When running the process agent daemon **nco_pad**, you must use the **–keyfile** command-line option to specify the file path and file name of the key file.



You might also use other property values within files. These examples show some of these values.

To run in FIPS 140-2 compliance, use the **ConfigCryptoAlg** property in your files, as in following example.

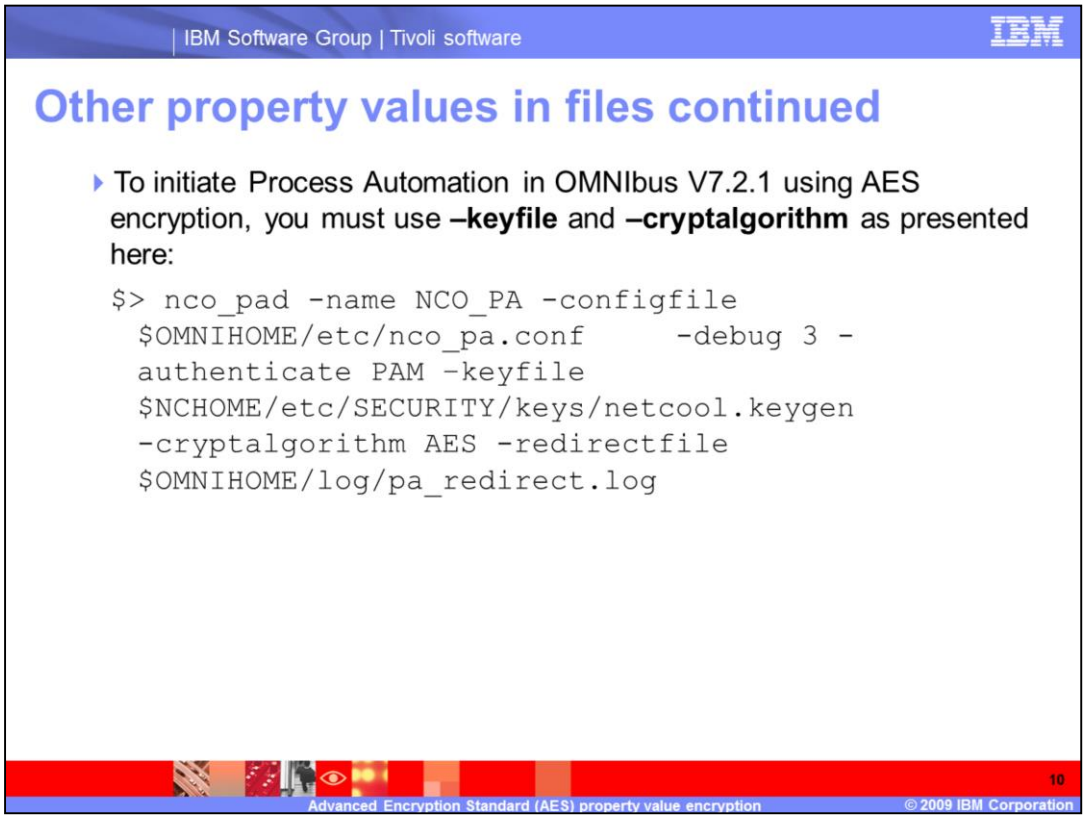
`ConfigCryptoAlg: AES_FIPS` in files

`And -cryptalgorithm 'AES_FIPS'` in the nco_pad command line

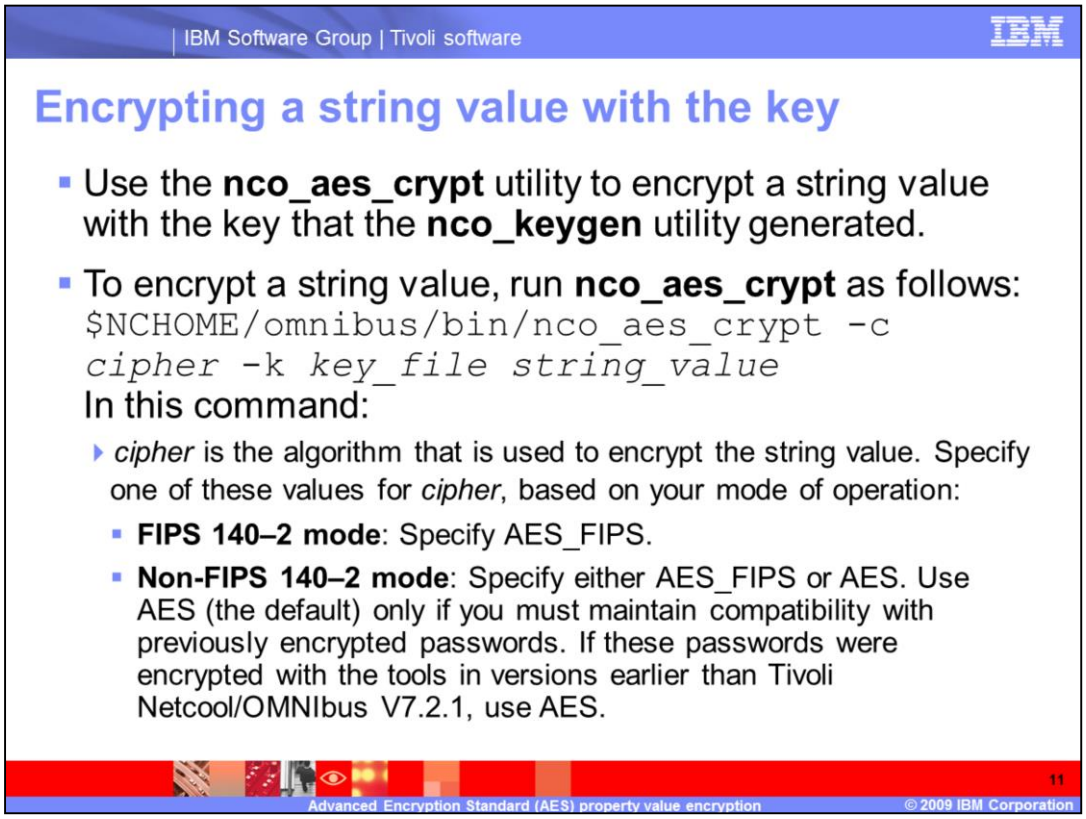
You might set the **PasswordEncryption** property within your ObjectServer's property file in one of the following two ways:

At ObjectServer creation by using the **`nco_dbinit -pwdenc AES -server NCOMSA`**

or within the existing ObjectServer's property file. Use the **`PasswordEncryption: 'AES'`** `value.`



To initiate Process Automation in OMNIbus V7.2.1 using AES encryption, you must use **–keyfile** and **–cryptalgorithm** as presented here.



Use the **nco_aes_crypt** utility to encrypt a string value with the key that the **nco_keygen** utility generated.

To encrypt a string value:

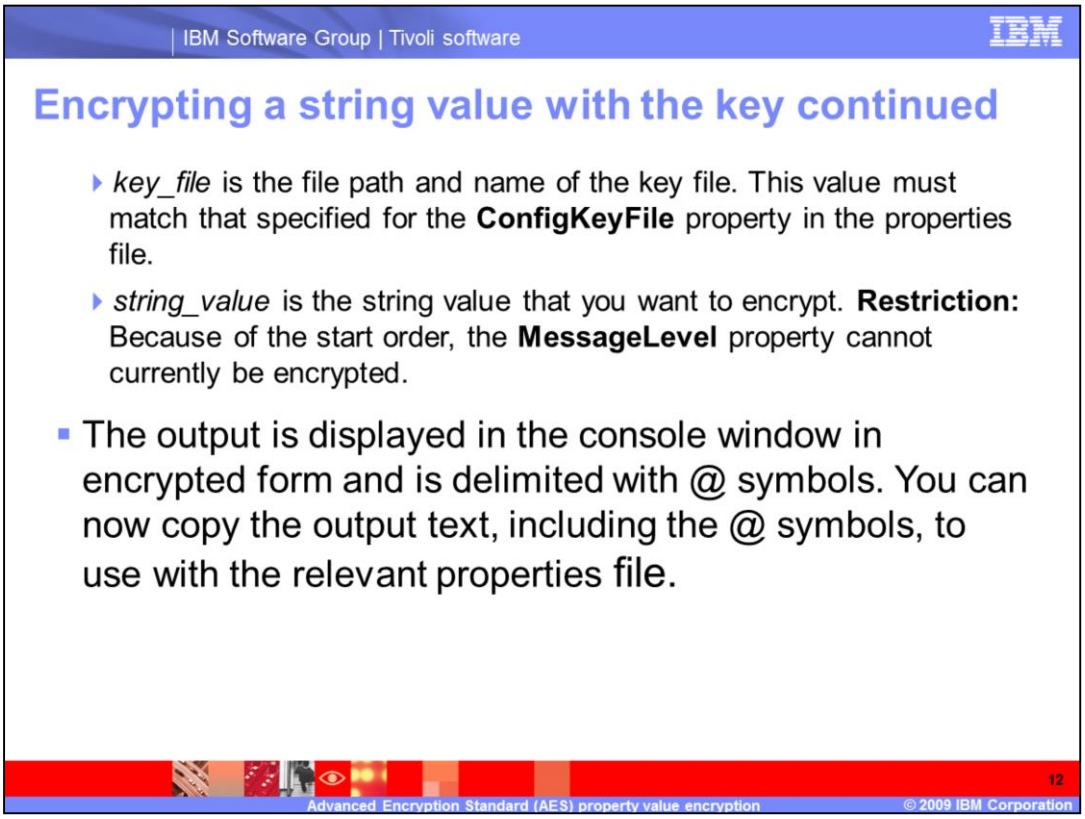
Run **nco_aes_crypt** as follows: $NCHOME/omnibus/bin/nco_aes_crypt -c *cipher* -k *key_file string_value*

In this command:

cipher is the algorithm that is used to encrypt the string value. Specify one of these values for *cipher*, based on your mode of operation:

FIPS 140–2 mode: Specify AES_FIPS.

Non-FIPS 140–2 mode: Specify either AES_FIPS or AES. Use AES (the default) only if you need to maintain compatibility with passwords that were encrypted using the tools provided in versions earlier than Tivoli Netcool/OMNIbus V7.2.1.

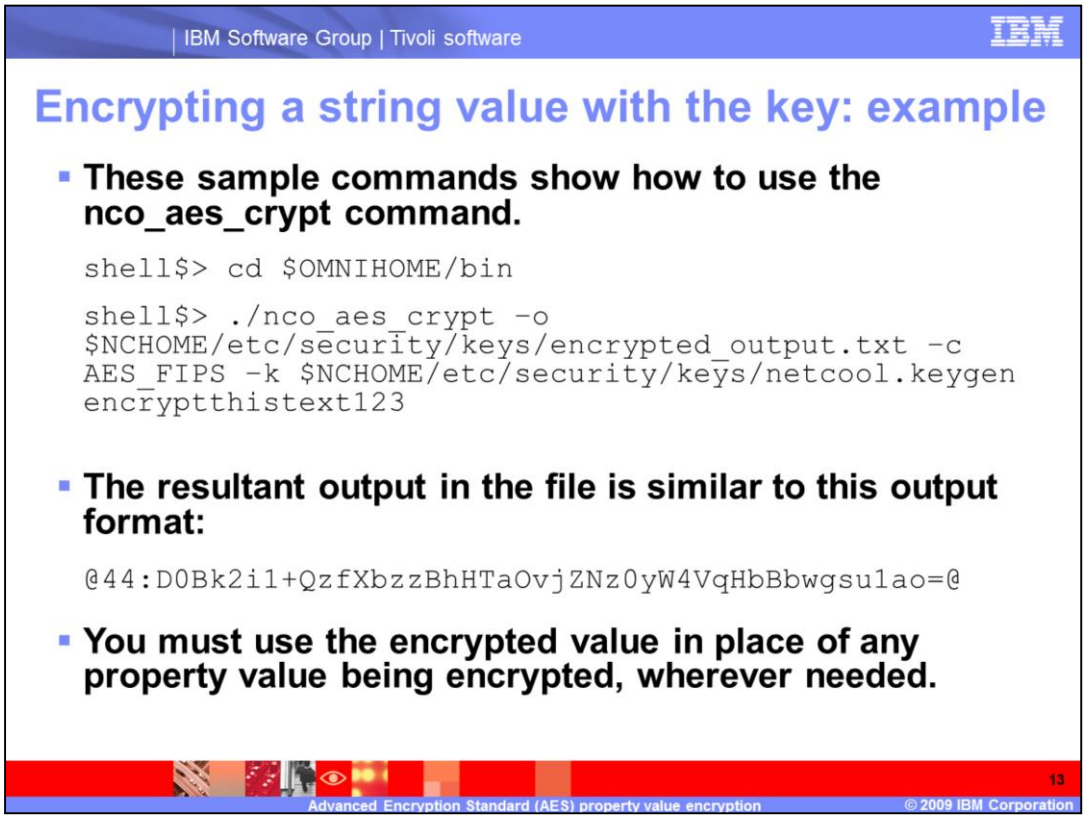


The command parameters continued from the previous slide also include values:

key_file which is the file path and name of the key file. This value must match that specified for the **ConfigKeyFile** property in the properties file.

string_value which is the string value that you want to encrypt. **Restriction:** Because of start order, the **MessageLevel** property cannot currently be encrypted.

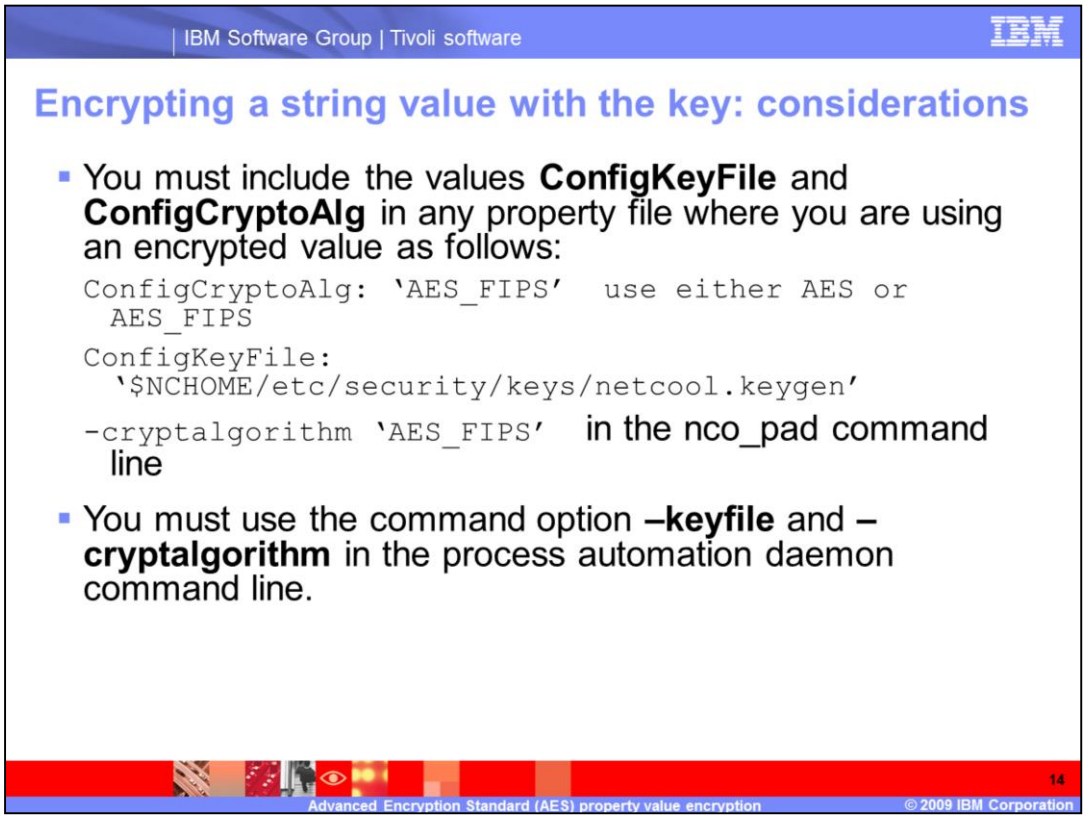
The output is displayed in the console window in encrypted form and is delimited with @ symbols. You can now copy the output text, including the @ symbols, to use with the relevant properties file.



These sample commands show how to use the **nco_aes_crypt** command.

The resultant output in the file is similar to this output format.

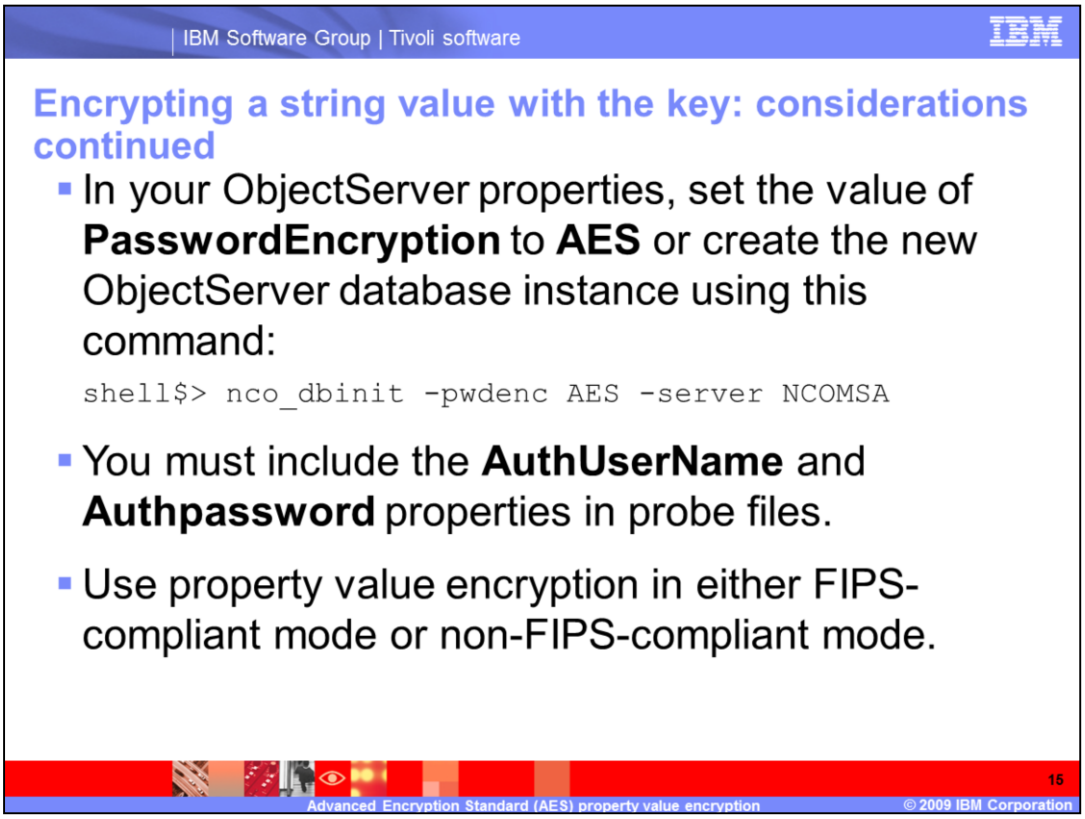
You must use the encrypted value in place of any property value being encrypted, wherever needed.



A few consideration to take note of are:

You must include the values **ConfigKeyFile** and **ConfigCryptoAlg** in any property file where you are using an encrypted value.

You must use the command option **–keyfile** and **-cryptalgorithm** in in the process automation daemon command line.



In your ObjectServer properties, set the value of **PasswordEncryption** to **AES**, or create the new ObjectServer database instance using the nco_dbinit command.

You must include the **AuthUserName** and **Authpassword** properties in probe files.

Use property value encryption in either FIPS-compliant mode or non-FIPS compliant mode.

Training roadmap for *Tivoli Netcool/OMNIbus*

http://www.ibm.com/software/tivoli/education/edu_prd.html

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:

Tivoli

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

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.