Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Pervasive Encryption on z/OS

CODE:	LENGTH:	PRICE:
ESS10G	24 Hours (3 days)	€2,340.00

Description

Organizations are compelled to find effective and cost-efficient data security solutions.
Encryption is one of the technologies that enables organizations to reduce the cost, impact and even likelihood of a breach.
Encrypting data can help companies meet the stringent mandates of the GDPR, HIPAA and other mandates.
IBM z15 has been designed for pervasive encryption, enabling organizations to encrypt 100% of an organizations IBM Z critical business data in-flight and at-rest, with no application changes and no impact to SLAs. Encrypting only the data required to meet compliance mandates should be considered a minimum threshold, not a best practice. IBM z15 makes pervasive encryption the new standard in data protection and the foundation of a larger data security and protection strategy.
z/OS is designed to provide new policy-based encryption options that take full advantage of the improvements in the z15 platform.
These new capabilities include:
Data set encryption, which is one aspect of pervasive encryption, provides enhanced data protection for many z/OS data sets gives users the ability to encrypt data without needing to make changes to applications to embed encryption APIs within applications.
New z/OS policy controls which make it possible to use pervasive encryption to protect user data and simplify the task of compliance for many z/OS data sets, zFS file systems, and Coupling Facility structures.
Pervasive encryption for IBM Z® is a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption and reduce costs associated with protecting data.
In this course you will learn how to implement Pervasive Encryption in your z/OS installation. The course explores in detail, the various technologies that are involved in z System and z/OS Cryptographic Services, ICSF, RACF and DFSMS access method Services.
In the hands-on exercises, you begin with the setup of your hardware crypto environment (CCA crypto express and CPACF), then you will load and activate your AES master keys, setup ICSF and its Key datasets (CKDS PKDS TKDS), then define your data encryption keys, activate your data set encryption policy, and encrypt your data sets and zFS filesystems.
These exercises reinforce the concepts and technologies being covered in the lectures.

Objectives

After completing this course, you should be able to:

- Describe the components of Pervasive Encryption on z/OS
- Explain the role of encryption for data protection

2

- Implement hardware crypto on your z System
- Load and activate AES Master Keys
- Implement and start ICSF
- Understand the differences between secure keys clear keys and protected keys
- Describe how are key values used for encryption and decryption
- Generate, maintain and manage Keys
- Setup access to key labels
- Setup policy to supply key label (RACF SMS JCL)
- Access data in encrypted data sets
- Create encrypted data sets - Supplying key labels
- Convert existing data sets to encryption
- Verify encryption status
- Encrypt Data in Transit
- Encrypt Data at Rest
- Manage data sets, data keys, and key labels

Audience

This class is intended for z/OS system programmers and security specialists in charge of designing, implementing and monitoring Pervasive Encryption on z/OS.

Prerequisites

- General z/OS knowledge, including basic UNIX System Services skills
- Basic knowledge of RACF
- Curriculum relationship o [ES66G]

Programme

- Describe the components of Pervasive Encryption on z/OS
- Explain the role of encryption for data protection

2

- Implement hardware crypto on your z System
- Load and activate AES Master Keys
- Implement and start ICSF
- Understand the differences between secure keys clear keys and protected keys
- Describe how are key values used for encryption and decryption
- Generate, maintain and manage Keys
- Setup access to key labels
- Setup policy to supply key label (RACF SMS JCL)
- Access data in encrypted data sets
- Create encrypted data sets - Supplying key labels
- Convert existing data sets to encryption
- Verify encryption status
- Encrypt Data in Transit
- Encrypt Data at Rest
- Manage data sets, data keys, and key labels

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.