CA ARCserve Backup r12 - Data Encryption

Data security is one of the major challenges that companies face today. Protecting critical data and applications to meet business needs for access and availability is vital to success in the marketplace. All this while protecting company property, public image, and complying with Government regulations on information availability and security.

CA ARCserve Backup r12 addresses these challenges by providing a FIPS compliant backup data protection solution that uses AES (Advanced Encryption Standard) to encrypt data, which is more secure than DES (Data Encryption Standard) and complies with the Government regulations to protect electronic data. Customers have a choice to encrypt data at multiple levels without impacting production server performance, increase backup window, or tape media usage. For companies that send tapes offsite—tapes that often times include company or customer confidential information—CA ARCserve r12 offers the ability to encrypt at the tape level.

**Overview**

CA ARCserve provides the flexibility to use encryption to protect sensitive data during various stages of the backup process.

You can encrypt data in a backup job using one of the three options:

- Encryption at the agent
- Encryption at the CA ARCserve server during the backup
- Encryption at the CA ARCserve server during migration (for staging job).

**Benefits**

- Secured data
- FIPS compliant
- Secured migration: CA ARCserve provides secure Windows client agents that use a 256-bit AES algorithm provided in the RSA BSAFE cryptographic library for all encryption purposes.
- Software/Hardware encryption based on final destination device for Regular/Data migration job.

**Install/Configure**

The Data Encryption feature is installed as part of the CA ARCserve r12 Enterprise Module installation.

**How the feature works**

To enable Data Encryption, from the Backup Manager window, click Options, Backup Media, and select the encryption type and specify encryption password. During the restore operation, provide the same encryption password to retrieve the data. Compression is optional and done before encryption.

CA ARCserve r12 detects if the hardware device is capable of data encryption. If the hardware device is encryption enabled, hardware encryption takes precedence over software encryption and CA ARCserve backup server uses hardware encryption.

**Data Encryption at the Agent**

CA ARCserve r12 enables you to encrypt data at the CA ARCserve Backup agent prior to the actual backup. The advantage of this method is that the data is encrypted before it is transferred from one location to another over the wire. However, this method adds CPU cycles on the machine where the engine is running. Encryption will be done either at the agent or on the tape drive but not both. If both the options are chosen, agent level encryption will be honored.

**Data Encryption at the Server during Backup**

The un-encrypted data is transferred from the agent to the CA ARCserve Backup server. The server performs software encryption before transferring the data to the hardware device. This encryption mechanism is faster and does not interfere with the backup window. However, if the hardware device is encryption enabled, hardware encryption takes precedence over software encryption.
Data Encryption at the Server during Migration

The un-encrypted data is transferred during backup of a staging job from the agent through the CA ARCserve Backup server to the staging device. The staging device can either be a disk, tape, or Virtual Tape Library (VTL). With this enhancement, users will be able to define encryption parameters that would be applied by CA ARCserve during scheduled migration of the backed up data from the staging device. When encryption parameters are set and hardware encryption capabilities are detected, the hardware encryption feature will be automatically enabled on the device. This will offload the encryption overhead from your Backup server.

Frequently Asked Questions

Q: Is CA ARCserve Backup FIPS Compliant?
A: Yes, CA ARCserve Backup uses FIPS-compliant algorithms to back up and restore the data including username and password credentials.

- If you choose to encrypt your data during backup to a disk or tape, the algorithms used to encrypt this data will be FIPS-compliant.
- During backup, the username and password is sent to the CA ARCserve Backup server agent (running on the server to be protected). This username and password will be encrypted using FIPS-compliant algorithms and transferred to the agent.

Q: What are the agents provided by CA ARCserve that use FIPS-compliant algorithms to support data encryption?
A: The agents provided by CA ARCserve that use FIPS-compliant algorithms to support data encryption are Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint, and CA XOsoft Replication.

Summary

The CA ARCserve Backup r12 Data Encryption feature enables you to encrypt data at multiple levels without impacting production server performance. The data can be encrypted at Agent/Server/Hardware level.

To get maximum value from your investment in CA software, CA Education can help you get the right training for your unique challenges. Visit http://ca.com/education for additional information.