12.1 Planning for encryption

Data-at-rest encryption is a powerful tool that can help organizations protect the confidentiality of sensitive information. However, encryption, like any other tool, must be used correctly to fulfill its purpose.

Multiple drivers exist for an organization to implement data-at-rest encryption. These can be internal, such as protection of confidential company data, and ease of storage sanitization, or external, such as compliance with legal requirements or contractual obligations.

Therefore, before configuring encryption on the storage, the organization defines its needs and, if it is decided that data-at-rest encryption is required, includes it in the security policy. Without defining the purpose of the particular implementation of data-at-rest encryption, it is difficult or impossible to choose the best approach to implement encryption and verify whether the implementation meets the set of goals.

The following items are worth considering during the design of a solution that includes data-at-rest encryption:

- Legal requirements
- Contractual obligations
- Organization's security policy
- Attack vectors
- Expected resources of an attacker
- Encryption key management
- Physical security

Multiple regulations mandate data-at-rest encryption, from processing of Sensitive Personal Information to the guidelines of the Payment Card Industry. If any regulatory or contractual obligations govern the data that is held on the storage system, they often provide a wide and detailed range of requirements and characteristics that need to be realized by that system. Apart from mandating data-at-rest encryption, these documents might contain requirements concerning encryption key management.

Another document that should be consulted when planning data-at-rest encryption is the organization’s security policy.

The outcome of a data-at-rest encryption planning session answers the following questions:

1. What are the goals that the organization wants to realize by using data-at-rest encryption?
2. How will data-at-rest encryption be implemented?
3. How can it be demonstrated that the proposed solution realizes the set of goals?

12.2 Defining encryption of data at-rest

Encryption is the process of encoding data so that only authorized parties can read it. Secret keys are used to encode the data according to well-known algorithms.

Encryption of data-at-rest as implemented in IBM Spectrum Virtualize is defined by the following characteristics:

- *Data-at-rest* means that the data is encrypted on the end device (drives).
- The algorithm that is used is the Advanced Encryption Standard (AES) US government standard from 2001.