IBM Security Guardium Key Lifecycle Manager

Business data is growing at exponential rates, driving the demand to secure data on-premises and in the cloud. Enterprises have responded by implementing encryption at various layers – in hardware, on files and in applications. This response can result in encryption silos with inconsistent approaches to managing encryption keys. In some cases, there is no formal key management process in place. Whether key management is fragmented or non-existent, organizations are at risk of losing control of their data. They need a solution that can integrate with other key managers and self-encrypting devices – using standard protocols – and can centralize encryption key lifecycle management.

Deploy a simple solution to a complex problem

IBM Security Guardium Key Lifecycle Manager provides a simple solution to the complex problem of key management. Encryption keys have their own lifecycles that are separate from the data they're protecting. Guardium Key Lifecycle Manager can help manage key lifecycle processes from initialization and activation through rotation and deletion, allowing organizations to simplify and automate what can be manual tasks, and thus, reduce operational costs.

As more data is stored across the hybrid multicloud environment, there are growing risks of data loss or compromise. To reduce this risk, data should be encrypted, and the organization should control the keys. Guardium Key Lifecycle Manager helps ensure sensitive information is protected in the event that encrypted data stores are misplaced, misused or stolen.

Highlights

- Modernized architecture for container deployment
- KMIP, IPP and REST-based key exchange support
- Simplified and automated key management from a centralized location
- Security risk mitigation that can help address industry and government regulations

Centrally manage encryption keys

Guardium Key Lifecycle Manager serves keys at the time of use from a secure, centralized location that stores the key materials. This is made possible by its support of proprietary and internationally standardized protocols for serving symmetric and asymmetric keys that include Key Management Interoperability Protocol (KMIP), IBM Proprietary Protocol (IPP) and Representational State Transfer (REST), which allow Guardium Key Lifecycle Manager to manage encryption keys for IBM and non-IBM solutions. For organizations that want centralized control and policy-driven key management, Guardium Key Lifecycle Manager offers consolidated management of keys across domains and integrates well into existing security-team methodologies.

Guardium Key Lifecycle Manager provides support for the encryption keys of a wide range of solutions, a sampling of which can be found here: https://www.ibm.com/support/pages/ibm-security-key-lifecycle-manager-supported-storage-and-non-storage-devices

Take advantage of strong access management and security

Guardium Key Lifecycle Manager enables organizations to define which administrators can perform custodial actions on keys and to limit permissions to only the functions users require to perform their jobs. These role-based access control features enable segregation of duties, mapping of permissions for actions performed against objects and enforcement of data isolation and security. Permitted users can also group devices into separate domains, and by default, the groups of devices have access only to the encryption keys defined within their group.

Prior to managing its encryption keys, each device is registered with Guardium Key Lifecycle Manager. Each time an encryption device reconnects to request a key, Guardium Key Lifecycle Manager verifies its identity and cryptographically authenticates using the device's identifying certificate. Any unknown device is rejected or placed into a queue to be approved by the administrator. With this strategy, a rogue device cannot be deployed on the network and used to intercept keys.

In addition to strong authentication, there is also strong security between the data encryption device and Guardium Key Lifecycle Manager. Temporary session keys are used to encrypt the encryption key and all of the traffic to the device. This approach to encryption can improve data security while simplifying encryption key management. The impact on performance is minimal, and each encryption solution performs cryptographic tasks instead of reaching across the network.

For scenarios in which keys are needed more frequently, Guardium Key Lifecycle Manager works with the organization's existing high-availability and disaster-recovery solutions to create and replicate keys. Furthermore, it has Multi-Master capabilities for real-time synchronization of up to 21 instances across data centers and environments.

While the cryptography inside of Guardium Key Lifecycle Manager is validated to FIPS 140-2 Level 1, users also have the option to leverage FIPS 140-2 Level 2- or 3-validated hardware to enhance key security. Guardium Key Lifecycle Manager can be deployed with an optional hardware security module (HSM) to store the master key that is used to protect all keys stored in Guardium Key Lifecycle Manager. This capability can be enabled for installs with existing data or for new installations of Guardium Key Lifecycle Manager.

Simplify key configuration and management tasks

Guardium Key Lifecycle Manager provides an easy-to-use, web-based GUI that helps simplify key configuration and management tasks. With this GUI, administrators can easily create keys, assign keys and manage the key lifecycle from a centralized console.

Once installed, the GUI allows administrators to perform basic local key lifecycle management and offers not only configuration and setup tools, but also audit and compliance support. The software provides three ways to add encryption-enabled devices: Auto-acceptance of incoming devices, approval of devices that requires administrators to select and accept from a pending device list or manual addition of devices for extra security.

Guardium Key Lifecycle Manager also provides numerous methods for key backup and recovery in case of disaster. Administrators can configure rules for automated rollover of groups of keys so that new encryption keys are used automatically based on a configurable schedule. In this way, administrators can limit the amount of data encrypted with particular keys, minimize exposure when a key is compromised and perform cryptographic erasure of data by deleting relevant keys when data is set to expire. The end result is the ability to configure automated key assignments over time such that the operations team has to infrequently interact with key management.

Expedite deployment with Wizard-based assistance

Guardium Key Lifecycle Manager uses a wizard-based guide to help administrators through a series of simple, task-based screens that demonstrate key and device creation and the handling of new device requests. Administrators can also configure different devices to use certain communication protocols such as KMIP.

Once registered, encryption devices appear in the Guardium Key Lifecycle Manager key administration section and are ready for use as a secure endpoint. The keys associated with the devices can then be managed through the GUI, including updating, expiring or destroying the keys. The Guardium Key Lifecycle Manager key administration welcome page provides critical notices to administrators including information about last backups and available protocols.

Benefit from lightweight, flexible deployments

Guardium Key Lifecycle Manager is an application that can be deployed on a variety of operating systems including Windows, Unix, Linux, and IBM mainframes. Its design and architecture do not require extensive RAM or processing resources; in fact, the solution can typically be deployed with 8 GB of RAM and a dual processor core.

Thanks to the application’s small footprint and the ability to be deployed as a virtual machine, a container (Red Hat OpenShift Container or Kubernetes) or on bare-metal, organizations are easily able to manage multiple instances of Guardium Key Lifecycle Manager for redundancy and high availability or alignment with the organizational structure.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security

IBM

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid, multicloud environments. Visit ibm.com/security/data-security/guardium