cpl.thalesgroup.com

THALES

CipherTrust Manager and IBM N Series: Securing Network-Attached Storage

The Challenge

Today's enterprise often finds itself needing to manage several encryption solutions that have proliferated across multiple tiers and vendor platforms, and have been deployed within primary, secondary, and even cloud-based data centers. This fragmented approach to data security has left many organizations in a management and operational quandary. Successfully implementing encryption is fundamental to addressing regulatory mandates, regularly passing security audits, and protecting sensitive information. However, as the number of encryption solutions increases, so too does the number of encryption keys, key stores, and associated access policies that must be managed. Security teams struggle to contend with the administrative effort of managing not only encryption deployments but also the associated key lifecycle operations. In order to cost-effectively support such an environment and bring it into regulatory compliance, centralized enterprise key management must be part of the solution.

The Solution

Enterprise key management—that is, a centralized repository that manages all encryption keys and data access policies across the enterprise—is an effective means to ensure that encrypted data is protected against unauthorized access while also simplifying the management of associated keys for all deployed encryption solutions. Thales CipherTrust Manager simplifies the operational challenges of managing encryption keys, making sure keys are secure and information is always available to authorized users within your IBM N Series storage infrastructure. As the use of encryption proliferates throughout an organization, security teams must be able to easily scale their key management. With CipherTrust Manager, administrators can simultaneously manage keys associated with the Thales data encryption solutions as well as appliance and other KMIP-based solutions, such as encrypting SAN switches and tape libraries. Security teams gain the critical key management capabilities they need to secure physical, virtual, and private cloud-based environments while enforcing security policies surrounding access and use.

With IBM N Series and Thales, you can enjoy the benefits of a network storage environment that delivers the unique features of the clustered Data ONTAP® operating system, combined with CipherTrust Manager enterprise key management, to make sure that your encrypted data remains available at all times for your users and important workloads.

With clustered Data ONTAP, you have access to IBM N Series storage efficiency technologies, including Snapshot copies; thin provisioning; FlexClone®, SnapMirror, and SnapVault® technologies; deduplication; compression; RAID-DP® technology; and flash, using the A and G model families of storage controllers. CipherTrust Manager maintains data confidentiality on IBM N Series A and G models through efficient centralized key management and by enforcing customized security policies surrounding data access.

This combination of a modern storage infrastructure and Thales key management delivers the peace of mind that your data and its encryption keys are protected against unauthorized access while simultaneously making the most efficient use of your storage investments.

Key Features

Centralize Management of Encryption Keys

- Centralize and simplify key management for your entire IBM N Series infrastructure while improving compliance and auditability.

Enable Multi-Tenant Data Isolation

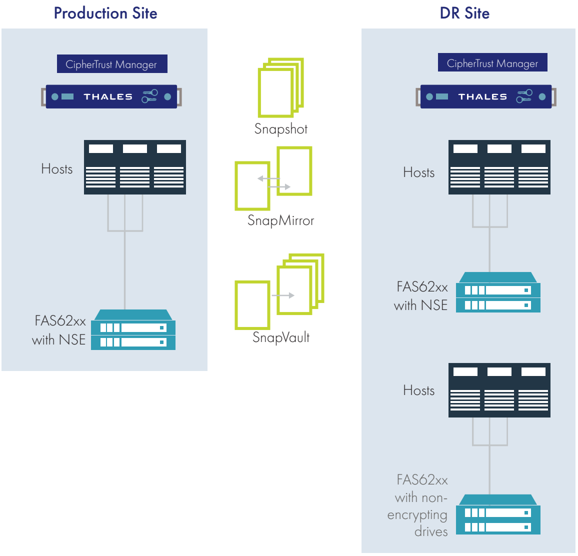
- Leverage shared resources while securing data by business policy to segregate data for multiple departments, business units, or customers.

Achieve High Availability

- Cluster multiple CipherTrust Manager appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Enable Auditing, Logging, and Alerting

- Improve regulatory compliance for your entire IBM N Series environment with a non-repudiative audit trail.



Centralize Management of Encryption Keys

Disparate encryption solutions lead to key management silos, each with its discrete enforcement policy. CipherTrust Manager's support for the KMIP protocol enables it to centralize and simplify key management for your entire IBM N Series infrastructure, including encrypting SAN switches and tape libraries while removing the challenge of ongoing maintenance, management, and auditability associated with disparate encryption solutions.

Ensure Root of Trust

Distributed or cloud-based storage can make data access control more challenging. Meeting compliance mandates in these environments is greatly simplified through verifiable and auditable enterprise key management. Data may reside locally, remotely, or virtually within your IBM N Series infrastructure or private cloud. However, the keys and user access controls are secured within CipherTrust Manager, which remains under your security team's control, not the storage administrators.

Enable Multi-Tenant Data Isolation

In multi-tenant or private cloud environments, where storage is shared across your IBM N Series infrastructure, granular key administration allows for the co-mingling of data without exposure to unauthorized users. CipherTrust Manager enables granular user authorization based on defined access and usage policies and can automatically retrieve administrator, security, and user access controls from existing LDAP or Active Directory services.

Enable Separation of Administrative Duties

CipherTrust Manager supports granular authorization, enabling constraints to be placed on specific key permissions to protect against insider threats through segmented key ownership based on individuals or group owners. Ongoing management of your IBM N Series storage occurs as always; however, storage administrators cannot gain access to sensitive data unless they are also entrusted by policy with access to the encryption keys.

Benefits of CipherTrust Manager in IBM N Series Storage Environments

Maximize Security

- CipherTrust Manager centralizes all key management activities, including key signing, role-based administration, quorum control, and the backup and distribution of encryption keys enterprise-wide. For sensitive security operations, you can stipulate multiple credential authorization from multiple administrators.

Resiliency and High Availability

- Multiple CipherTrust Manager appliances can be clustered for high availability, with configuration information replicated instantly between members to dramatically improve failover capabilities and fault resiliency for geographically dispersed data center deployments. CipherTrust Manager clusters can operate in both Data ONTAP 7 mode or clustered Data ONTAP environments.

Auditing, Logging, and Alerting

- CipherTrust Manager's built-in auditing, logging, and alerting functions facilitate regulatory compliance for your entire IBM N Series environment. All keys, certificates, and passwords are securely managed, key ownership is clearly defined, and key lifecycle management is logged to provide a non-repudiative audit trail.

Simplified Key Destruction

- Centralized key management simplifies disposing of keys when data is retired or replaced, or the integrity of the key has been weakened or compromised.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us