Intelligent Data Security for Mission-Critical IT

The Pivot3 hyperconverged infrastructure (HCI) software platform delivers a comprehensive set of data security capabilities to increase your security posture and ensure compliance with your industry's information security regulations. Data security management is integrated into the Pivot3 software platform's Intelligence Engine, which provides a simple, policy-based approach to encryption and key management.

COMPREHENSIVE DATA AT REST ENCRYPTION

FLEXIBLE, SECURE MULTI-TENANCY

SIMPLE, POLICY-BASED MANAGEMENT

INTEGRATED KEY MANAGEMENT

Comprehensive, Low Overhead Data at Rest Encryption

Pivot3 encrypts user and application data at a system-, volume- or VM-level to provide comprehensive security. A robust Advanced Encryption Standard (AES) 256-bit algorithm is used to ensure that maximum levels of military-grade security are applied to the data and in accordance with National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) 140-2 standard. The encryption process has low overhead and minimal performance impact (less than 5%) through tight integration with the Intel® AES New Instructions (Intel® AES NI) set that accelerates the encryption of data in the Intel® Xeon® processor family. By combining more intelligent data protection with Pivot3 patented erasure coding and faster, more comprehensive data security, IT can now deliver efficient and pervasive data protection and encryption.

Flexible, Secure Multi-tenancy

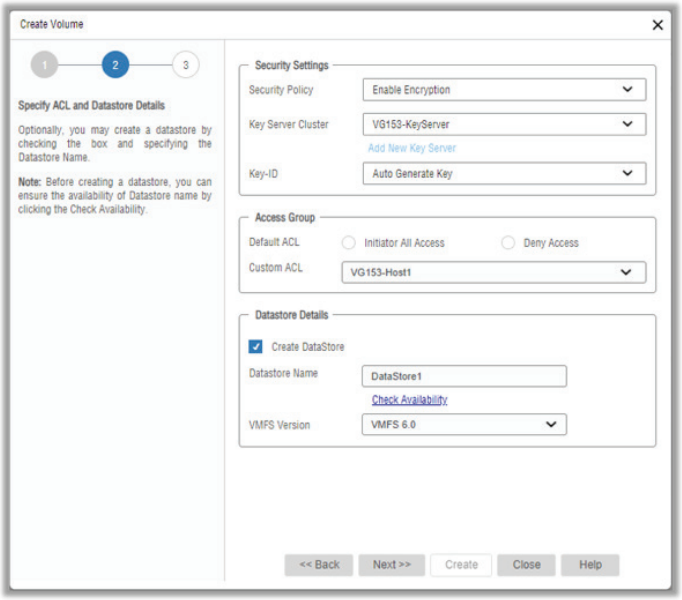
With close to 75% of security breaches, malicious, accidental or otherwise, coming from within the network, it is critical to have control and insight to who has access to data. By providing different data owners with different encryption keys, security can be maintained even if multiple tenants use the same HCI system. A series of Role-Based access control features are also available to help IT administrators and security managers mitigate threats from unauthorized access. These include "Least Man Privileges" where unless a user has been given specific authorization, it is assumed that they have the lowest level of privileges in managing the system and "Two-Man Authentication" where certain actions can be escalated up the management chain for approval before the system will carry them out.

With flexible multi-tenancy capabilities, you can consolidate multiple users and organizations on one Pivot3 HCI system and still maintain compliance boundaries where unauthorized actions can be stopped before they take place. Additionally, Pivot3's advanced and detailed logging capabilities provide a level of detail deemed suitable by NIST, HIPAA, GDPR and other standards for an audit trail, meaning that all audits will be performed quickly, efficiently and effectively.

Simple, Policy-Based Management

Policy-based management is a standard capability in the Pivot3 Intelligence Engine, a core foundation of the Pivot3 software platform. Encryption and key management are also managed using this simple, policy-based paradigm. This simplifies the management of the environment as it scales and simplifies the deployment process of sensitive or regulated workloads.

SECURITY ENABLED BY SIMPLE POLICY SELECTION FOR ENCRYPTION AND KEY MANAGEMENT



Create Volume

Specify ACL and Datastore Details

Optionally, you may create a datastore by checking the box and specifying the Datastore Name.

Note: Before creating a datastore, you can ensure the availability of Datastore name by clicking the Check Availability.

Security Settings

Security Policy: Enable Encryption

Key Server Cluster: VG153-KeyServer

Key-ID: Auto Generate Key

Access Group

Default ACL: ○ Initiator All Access ○ Deny Access

Custom ACL: VG153-Host1

Datastore Details

☑ Create DataStore

Datastore Name: DataStore1

VMFS Version: VMFS 6.0

Integrated Key Management

Encryption and key management can be applied at a system-, volume- or VM-level. Pivot3's integrated key management uses open standards Key Management Interoperability Protocol (KMIP) for strong security and interoperability with a variety of key managers. Finally, it is important in regulated environments to provide an audit trail to the necessary authorities, and should a breach occur, regardless of the source, there needs to be a forensically examinable audit trail of actions, authorizations and decisions made.

Additional System-level Security Features

Pivot3 has also implemented a series of system-based security features to aid in the undercover management of security at the device layer, enhancing those features at the data level. Mutual CHAP authentication allows secure connectivity and interaction between VM and storage volume. Integration with VMware single sign-on (SSO) promotes a simplification of user authentication, meaning that any potential loopholes between user interfaces are closed before they have a chance to be exploited. Having undergone the rigorous Common Criteria process, Pivot3 has been certified as a hardened and secure solution that meets the high standards for use in sensitive federal government environments, further attesting to the overall security robustness of the Pivot3 platform.

For more information, visit Pivot3.com