HITACHI
Inspire the Next

Hitachi Virtual Storage Platform Family: Security Overview

By Hitachi Data Systems

April 2015

Contents

Executive Summary

Data security now permeates every facet of the storage infrastructure. Whether data is stored as a file, a block or an object, it is now a foregone conclusion that security must be enforced throughout the entire storage ecosystem. Hitachi Virtual Storage Platform (VSP) midrange systems and Hitachi Virtual Storage Platform G1000 (VSP G1000), with our file and content offerings, provide the necessary components to address data security needs. An organization may need to address regulatory and compliance directives such as the Payment Card Industry Data Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Or, an organization may have general concerns regarding data security and the handling of sensitive information. VSP G1000 and the VSP midrange systems can help meet these challenges.

In addition to the technology involved with the security described below, Hitachi Data Systems leverages the Hitachi Incident Response Team (HIRT) for up-to-date notifications of and responses to the latest attack threats throughout our systems.

Hitachi Virtual Storage Platform G1000 Security Components

Hitachi Virtual Storage Platform family security architecture is made up of various components. These components are individually described in the following sections of this document.

Privileged User Access

Administration of VSP G1000 and VSP midrange systems is accomplished via Hitachi Command Suite (HCS) or Hitachi Storage Navigator. On VSP midrange systems it can also be completed through Hitachi Infrastructure Director (HID). HCS and HID are served from an external management appliance from VSP G1000, while Storage Navigator is hosted on the service processor internal to the VSP system. HCS, HID and Storage Navigator are storage management applications for your critical information. Therefore, it is an HDS best practice to locate the administrative IP interfaces of any storage management application or the device on a tightly controlled management network. This network is similar to a network where high-value management systems, such as firewall management consoles, are located. To further secure administrative access, HCS and Storage Navigator also support HTTPS for all management sessions.

Administrative Authentication and Authorization

VSP midrange systems and VSP G1000 support the ability to authenticate and authorize privileged users (also known as administrators) in two ways. Privileged end users can authenticate to the HCS, HID or Storage Navigator graphical user interface (GUI) or command line interface (CLI). This authentication is completed via a local shared security account database or through existing centralized authentication and authorization services that are present in the customer infrastructure. For authentication, the systems support the use of the RADIUS, LDAP and Kerberos protocols, which can leverage existing authentication infrastructure (for example, RADIUS, Microsoft® Active Directory® or LDAP). The protocols utilize various strong authentication mechanisms like multifactor or hard tokens (for example RSA SecurID Tokens). For authorization, VSP systems can leverage the existing group structures that exist in the organization's LDAP or Active Directory environment. All communications to and from the directory for authorization are secured using LDAP with StartTLS or LDAPS.

Role-Based Security

In order to prevent privileged users from making unauthorized changes to storage resources, VSP midrange systems and VSP G1000 have implemented a role-based security capability for both the GUI and CLI interfaces. This capability allows organizations to limit privileged user access to a predefined set of roles and assets for the VSP system. The roles can be tied back to the organization's directory infrastructure for centralized management of authorization data.

Fabric Security

Beyond traditional fabric security techniques that have historically lived in the SAN, the systems support two forms of port-level security as an extra layer of protection for critical data assets. The first of the two is logical unit number (LUN) security, where VSP systems can limit connections to a particular World Wide Name (WWN). Later, hosts of various types can be collected into host groups, which are then assigned to ports and LUN security is applied. Host groups can support multiple operating systems, depending on the organization's requirements.

In addition to LUN security, the systems also support the use of Fibre Channel authentication through its implementation of the Fibre Channel Security Protocol (FC-SP Auth A). An FC-SP implementation supports unidirectional and bidirectional switch to storage port authentication. This provision allows for an additional authentication layer in the fabric for critical applications and data paths. Support for FC-SP can also be found in the fabric infrastructure products from Hitachi data networking partners, including Brocade, Cisco and various host bus adapter (HBA) vendors.

Virus and Malware Protection

While virus scanning is not something that takes place at a block level, VSP family systems support the use of many commercially available virus scanners for the VSP service processor (SVP) appliance. While the SVP is a closed-management appliance, HDS does allow the use of qualified commercially available virus scanners on the SVP. These scanners are generally found as part of an organizations overall anti-virus and anti-malware infrastructure. For a complete list of supported anti-virus software contact your Hitachi Data Systems representative

Audit Logging

Traceability of security events on any device is a standard requirement in any regulated environment. VSP G1000 and the VSP midrange family are the fourth generation of Hitachi enterprise-class storage systems that support the use of external audit logging of security events. HDS was the first enterprise storage vendor to support this capability in 2005.

The Hitachi VSP family raises the bar by offering the first security audit logging in accordance with the recently updated Syslog RFCs (IETF 'Request for Comment' standards) to ensure security and reliable audit log transfers. This security audit logging capability takes advantage of TCP (Transmission Control Protocol) and TLS (Transport Layer Security) for reliable delivery and security of audit logging information. It keeps the information secure while it is transferred from the storage system to the organization's event management infrastructure. VSP G1000 and the VSP midrange family also maintain legacy support for UDP (User Datagram Protocol)-based audit logging, so it is backward compatible with previous generations of Syslog and legacy event management tools. Additionally there are improved audit logs for in-band command such as RAID manager and mainframe so that it is now human readable.

External audit logging is completed on an event-driven basis with time and date stamping. Additionally, for organizations that have a centralized time service, the VSP audit logging capability can leverage that service via NTP (Network Time Protocol).

Media Sanitization

When storage media are transferred, become obsolete, or are no longer usable or required by a storage system, it is important to ensure that the residual representation of existing data is deleted. It must not be easily recoverable. To assist organizations with such tasks, VSP systems support media sanitization through controlled overwrites of storage. This approach aligns with various sanitization standards, such as the U.S. Department of Defense (DoD) 5220.22-M. Data sanitization is applied at the LUN level. The process includes the capability to specify configurable overwrite patterns, the number of overwrite passes, and receive a file of results of the shredding operation. In addition to the sanitization results file, all-important sanitization events are recorded in the audit log as described earlier in this paper.

Resource Partitioning

Rather than using multiple storage systems for physical separation of resources, resource partitions allow for multiple users to safely coexist on a single storage system. Therefore, they avoid the risk of activities in one region affecting performance, availability or privacy in others. This functionality leverages the flexibility of the VSP systems, allowing IT organizations and storage service providers to implement consolidation strategies. But they do so in a manner that enables secure access for applications, storage administrators, applications and business units, while supporting mainframe and open systems environments simultaneously. Resource partitions can horizontally or vertically segment VSP storage resources, enabling management flexibility, while leveraging existing directory service infrastructure (AD/LDAP) for management access control.

Data-at-Rest Encryption

VSP G1000 and VSP midrange systems provide a performance-friendly AES-256-XTS encryption capability on the back-end I/O module. This capability protects data at rest on internal storage media (for example, hard disk drives and flash drives) and volumes attached to those directors. If data is encrypted, information leakage can be prevented when replacing the disk storage system or the drives in the disk storage system. Likewise, the VSP encryption capability provides an extra measure of protection and confidentiality for lost, stolen, or misplaced media that may contain sensitive information. It also provides a unique encryption key for each individual piece of media internal to the array.

The VSP encryption capability is configured and monitored through the GUI-based HCS and Storage Navigator management software. It provides role-based access control (RBAC) for the separation of duties including enabling/disabling of encryption as well as archiving encryption keys.

Key Management

Key management, especially for volume-based encryption, can be one of the more difficult aspects of data-at-rest encryption. As such, key management can become an impediment to using encryption, or worse, it can cause data loss due to operator error or lack of action.

Recognizing this situation and fully understanding the applicability to VSP family systems, Hitachi has implemented its encryption feature such that little human intervention is required. This approach helps ensure that data are not compromised due to key mismanagement. VSP family supports a simplified key management approach for key protection, backup and recovery for those organizations that do not have an existing key management infrastructure in place. For those organizations that have a formalized key management infrastructure already, VSP systems support the Key Management Interoperability Protocol (KMIP). The protocol supports generation, backup and recovery of data encryption keys, as well as trusted source operations, which will integrate with many key management products on the market today.

Secure Remote Support

When enabled, the Hi-Track Remote Monitoring system provides the remote support service and information transport function for HDS products as well as error analysis, case creation and error or information functions. It provides the above functionality for all HDS-serviced Hitachi products as well as a number of third-party products. HDS developed and maintains Hi-Track and provides device monitoring for potential error conditions and transfers relevant data immediately to the Hi-Track server at HDS. In addition to its reporting and notification functions, Hi-Track includes a customer-controlled option to grant service access to specific HDS support personnel. This secure remote support feature leverages a Hitachi remote access control center server within the customer LAN. All communications with the remote access control center server are secured using SSL/TLS in a firewall-friendly manner, and they are compatible with HTTP/S application proxies.

Third-Party Validation

While making claims about the security features and functions of a product is one thing, it is also incumbent on a vendor to demonstrate trustworthiness of their products. HDS demonstrates trustworthiness of its products by using vetted security technologies and methodologies as well as achieving product-based security certifications. VSP G1000 and VSP midrange family systems are in the process of achieving Common Criteria (ISO 15408) Certification at an Evaluated Assurance Level (EAL) 2+ and will be the fourth generation of Hitachi enterprise storage systems to do so. Additionally, VSP midrange and VSP G1000 systems are also being scheduled to undergo third-party validation of its encryption capabilities in the near future for FIPS 140-2 validation.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 96050-2639 USA
www.HDS.com community.HDS.com

Regional Contact Information
Americas: +1 408 970 1000 or info@hds.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hds.com
Asia Pacific: +852 3189 7900 or hds.marketing.apac@hds.com

WP-486-B J Harker April 2015