Hitachi Content Platform (HCP)

HCP Security Hardening Whitepaper

June 2020

Rev 1.0

Table of Contents

List of Figures

List of Tables

1. Executive Summary

This paper focuses on the numerous security features built into Hitachi Content Platform (HCP) cloud storage software to protect and secure data, access, and communications. These features are designed to help administrators and network engineers to deploy HCP in a way that minimizes vulnerabilities and threat exposure.

Functionally, HCP software may be summarized as a distributed data management layer able to virtualize pools of dissimilar storage, combine them into a single global namespace, and serve out thin provisioned virtual storage systems that speak both file and object protocols. The system enforces multitenancy and namespace isolation across these virtual storage systems to create virtual object stores that maintain separation between applications, users, data, and storage.

The software includes multiple layers of security that protect physical, network, tenant, administration, and data access. Other security features include use of certificates, data-in-flight encryption (DIFE), Internet Protocol (IP) whitelisting and blacklisting, data-at-rest encryption (DARE), and regular security scans.

Other security highlights include:

Administration Capabilities Separation: There are multiple administration domains, with segregation of roles and powers. Role-based access control (RBAC) administration scope is set independently at the system level or tenant level. Administrators have appropriate access to functionality, based on their role and scope.

Data Access Isolation: Data access is controlled by access-control lists (ACLs) in which the most restraining permission is enforced to avoid unauthorized access to data. ACLs control data access at an individual object level. ACLs provide more granular data access controls that limit the permissions granted to users or user groups, as well as the permitted operations.

Encryption: If enabled, HCP utilizes an Advanced Encryption Standard (AES)-256 block cipher with a key (or block) length of 256 bits. This is the cipher required for Federal Information Processing Standards (FIPS) 140-1 compliance. Data is encrypted when in flight and may be encrypted at rest.

User Authentication: In addition to local user accounts, HCP supports enterprise identity services: Microsoft Active Directory (AD), RADIUS and OpenStack Keystone.

Host-Based Firewalls: HCP follows security best practices and disables all external ports and processes that are not required by the software. Each HCP node runs a firewall that blocks all ports not associated with an active HCP service.

Server Certificates: HCP requires one server certificate (self-generated or uploaded PKCS12) for each defined domain to prove authenticity to clients.

Secure Remote Service: All remote service is performed using Secure Shell (SSH) and requires a 2048-bit key, which is available only to the Hitachi Vantara support organization. Organizations are empowered to disable this SSH access unless service is needed, at which time, SSH access can be enabled with the system-level administrator account.

Dedicated Management Network: Administrative tasks can be isolated on virtual LANs (VLANs) or physically separate Ethernet ports available on HCP servers.

2. Introduction

Hitachi Content Platform (HCP) is a distributed object store designed to provide a highly scalable, secure, cloud-enabled object repository platform capable of supporting multiple simultaneous applications. HCP takes a layered approach to security, ensuring the safety of data while restricting unauthorized access to it. This white paper summarizes the major areas of security in an HCP system and how they apply to object storage, access protocols, administration, and operations.

2.1 System Base Host-OS Hardening

The HCP software is developed to execute on a fully customized Fedora core operating system. To help increase its security, HCP engineers have worked to minimize the number of packages, services, and libraries by removing unused modules and application extensions. Command line access is similarly locked down, protected with large RSA keys (2048b), and only a minimum set of listening ports are enabled.

External security assessment and audits are periodically performed on HCP software. This includes network vulnerability scans using Nessus from Tenable Networks (www.tenable.com).

Other aspects of system hardening include the following elements:

- If a user is logged into the management console or the web portal and clicks on logout, all browser sessions will be terminated.
- HCP software makes no direct Structured Query Language (SQL) calls. All database functionality is passed through stored procedures to prevent SQL injection attacks.
- HCP is validated against an industry-standard vulnerability scanner to identify and resolve common security issues such as:
  - Weak Secure Sockets Layer (SSL) ciphers
  - Form injection attacks
  - Cross-site scripting (XSS) attacks
  - Cross-site request forgery (CSRF) attacks
- Software upgrades are online, fast, and simple, which facilitates rapid reaction to newly discovered security threats.
- Monitoring of system access attempts is done via the management console, so that an administrator can spot suspicious activity.

Assessments on Common Vulnerabilities and Exposures (CVE):

https://knowledge.hitachivantara.com/Support_Information/CVE_Security_Notices/CVE_Index_Page *[Note: Requires registration and login]*

2.2 Best Practice Security Deployment

The following list is a summary of best practices a consumer should take to ensure the highest level of security for the HCP platform.

Physical Security

- Limit physical HCP hardware access to a minimum set of trusted and qualified persons by locking the rack and the room in which it resides.
- Configure non-routable addresses for the back-end network, and prohibit any outside connections.
- Consider data-at-rest encryption to safeguard sensitive data from accidental disclosure.

Network Security

- Review port requirements and firewall unused ports.
- Disable SSH except during service periods.
- Disable Hypertext Transfer Protocol (HTTP) access except for debugging.
- Disable support for Transport Layer Security (TLS) 1.0 and 1.1.
- Establish multiple virtual (sub)-networks and/or utilize VLANs to logically segregate traffic types (e.g. Application, Tiering, Replication, Management).
- Ensure Network Time Protocol (NTP) and Domain Name Service (DNS) have authoritative sources.
- Explicitly limit namespace protocol access using allow/deny IP lists.

Authentication and Access Controls

- Use enterprise authentication.
- Enforce corporate password best practices (length, rotation, inactivity).
- Take a least-privilege approach to assigning role-based access controls.

Server Administration

- Keep HCP software updated to ensure latest bug fixes and Common Vulnerabilities and Exposures (CVE) protections.
- Mandate Hypertext Transfer Protocol Secure (HTTPS) is used for administrative functions and use allow/deny filtering of source IP addresses.
- Utilize roles to segregate system administration responsibilities.

3. System Hardening Topics

3.1 Physical Security

Physical security is primarily a customer issue. HCP can be deployed as either a hardware appliance or run in a virtualized environment. Regardless if HCP is a physical or virtual deployment, the customer should ensure that HCP is installed in their data center with the following in mind:

- Limited access to a minimum set of trusted and qualified persons.
- Configure non-routable addresses for the back-end network, and prohibit any outside connections
- Consider data at rest encryption to safeguard sensitive data from accidental disclosure

3.2 Network Security

Since data interaction with HCP is based on network communication, the primary concern should be to minimize the network-based vulnerability footprint. The following sections outline the network architecture of the multi-node solution and touch on the primary subjects of firewalls, usages of IP network security through TLS hardening, white/black lists, data access control, and general network services.

3.2.1 Architecture Overview

Users and applications access HCP using Ethernet technology. HCP software is installed on at least four servers with up to five physical Ethernet ports (IPv6 capable). ***Figure 1*** provides a sample HCP network diagram.

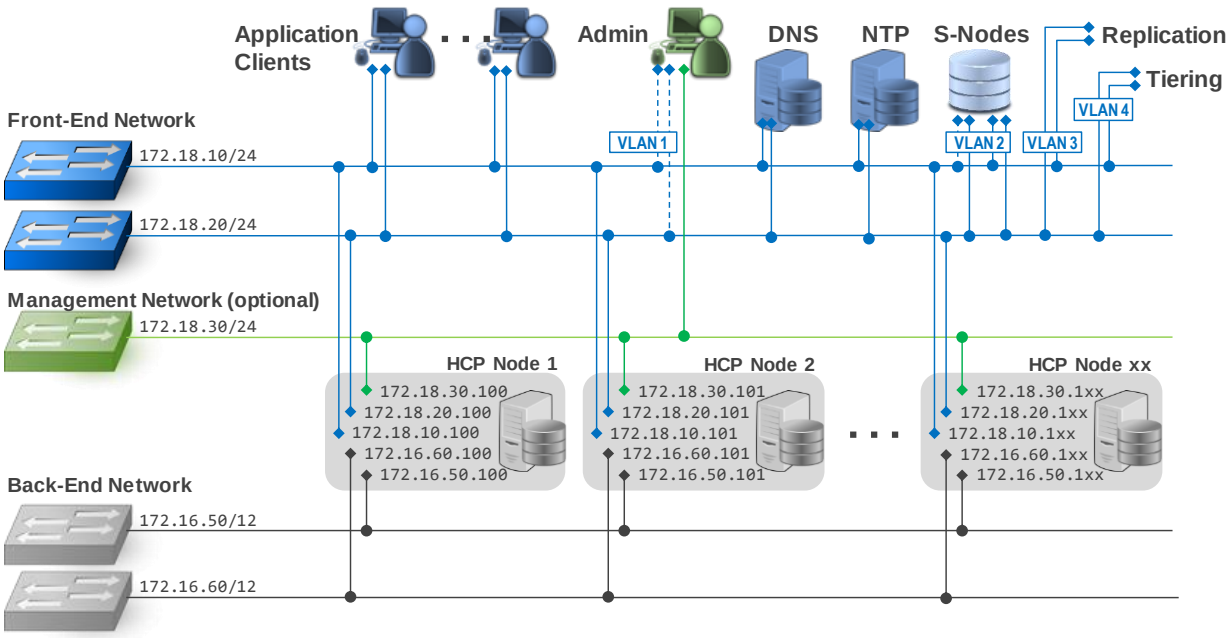

Figure 1. Hitachi Content Platform Network Diagram

At a high level, this diagram shows three main networks: Front-End Network (dual ported), Management Network, and Back-End Network. It also shows the expected external touch points for application clients, administrators, network services (DNS, NTP), HCP-S Series Nodes (a.k.a. S-Nodes) external storage, HCP replication, and HCP storage tiering.

Private Back-End Network: If HCP is a physical deployment, two switches along with all network cables are provided as part of an HCP appliance. If HCP is deployed in a virtualized environment, the customer is expected to provide a separate virtual switch. These networks carry traffic vital to internode communication. It is presumed that these switches and ports are physically/virtually protected within the data center to prevent unauthorized user access, tampering, and misuse. These network ports are reserved for HCP node members and should never be connected to other data center equipment. Follow these guidelines to ensure the security of this network:

- Configure non-routable addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) for the back-end network.

- Do not connect the HCP back-end switches to any other computer systems or networking gear.
- Limit physical access to the HCP nodes, switches, and storage arrays to authorized personnel.

Management Network: Some administrators prefer to run a management network that is separated from the data network. When initially installed, HCP administration activities occur on the front-end network with optional VLAN tagging, including *SSH, Simple Mail Transfer Protocol (SMTP), Syslog, Simple Network Management Protocol (SNMP), Messaging Application Programming Interface (MAPI)* and *web consoles* for system, tenant, and namespace management. HCP software can instead direct these management services to a previously unused physical/virtual 1Gb Ethernet port specific to HCP servers, creating a separate management network port. This redirection is **disabled** by default but can be enabled to improve the security of HCP administration via a dedicated, isolated, VLAN-capable network.

Front-End Network: This VLAN-capable network connects to a switch infrastructure provided by the customer organization. These networks carry application read/write traffic as well as management, tiering, and replication traffic. External communication with HCP is often managed through DNS, which round-robins client requests across all nodes to ensure maximum system throughput and availability. Versatile configuration options include VLAN tagging in native IPv4, native IPv6, or dual IPv4 and IPv6 modes across multiple virtual subnetworks.

Load Balancer: To add another layer of security and network traffic distribution, a load balancer (e.g. PulseSecure vADC) can be installed in front of HCP. From a security perspective, the load balancer can provide robust network routing and traffic filtering between any client applications and the HCP system. Additionally, the load balancer can be configured integrate with HCP to provide an I/O load-based distribution of requests to the HCP nodes.

3.2.2 Firewall Configuration

HCP deployment in the environment relies on two tiers of firewall to accomplish protection. The first level is accomplished via a firewall running in HCP, and the second is the data center firewall managed by the customer.

3.2.2.1 HCP Firewall

HCP maintains a firewall in each of the HCP nodes. This firewall is managed by the HCP software to ensure that only those necessary IP ports are available from external sources. The HCP administrator changes the firewall rules via high level configuration changes like enable/disable SSH, SMTP, SNMP, etc. To produce the smallest network vulnerability footprint, only enable those services that are required for the successful operation and management of HCP. These services will be discussed in later sections in this document.

3.2.2.2 Data Center Firewall

HCP nodes are typically deployed behind a corporate firewall; limiting access to the HCP front-end network remains an important part of the security strategy. Network engineers responsible for administrating the front-end switch may elect to restrict port utilization to a minimum set required by HCP software. ***Table 1*** presents a list of ports HCP might need during operation. The actual needs vary by specific deployment needs.

Table 1. Hitachi Content Platform Port Requirements

Port	Type	Direction	Default	Function	Used By
7	UDP	Inbound	Enabled	ICMP ECHO (ping)	Client Applications
22	TCP	Inbound	Disabled	Secure Shell version 2 (SSH2)	Client Applications
25	TCP	Both	Disabled	SMTP	Mail Servers
53	TCP/UDP	Both	Enabled	Domain Name Service (DNS)	DNS Servers
80	TCP	Inbound	Disabled	HTTP	Client Applications
123	TCP/UDP	Both	Enabled	Network Time Protocol (NTP)	NTP Servers
161	UDP	Inbound	Disabled	SNMP	Client Applications
162	UDP	Outbound	Disabled	SNMP Traps	SNMP Managers
443	TCP	Inbound	Enabled	HTTPS	Client Applications
514	UDP	Outbound	Disabled	System Log (syslog)	Syslog Servers
2001	TCP	Outbound	Disabled	Hitachi Device Manager (HDvM)	Monitoring Servers
5000	TCP	Both	Disabled	OpenStack Keystone	Identity Servers
5748	TCP	Inbound	Enabled	HCP Replication	HCP
8000	TCP	Inbound	Enabled	HCP Administration (HTTPS)	Client Browsers
8888	TCP	Inbound	Disabled	Web Search Console (HTTPS)	Client Applications
9090	TCP	Inbound	Disabled	Management API (HTTPS)	Client Applications
User set	TCP	Outbound	Disabled	RADIUS	Authentication Servers
Dynamic	TCP	Outbound	Disabled	Microsoft Active Directory (AD)	Authentication Servers
CIFS Protocol					
88	TCP/UDP	Inbound	Disabled	Kerberos (CIFS)	Authentication Servers
137	TCP/UDP	Inbound	Disabled	NETBIOS name service, CIFS	Application Servers
138	TCP/UDP	Inbound	Disabled	NETBIOS datagram service, CIFS	Application Servers
139	TCP/UDP	Inbound	Disabled	NETBIOS session service, CIFS	Application Servers
445	TCP/UDP	Inbound	Disabled	CIFS	Application Servers
NSF Protocol					
111	TCP/UDP	Inbound	Disabled	Portmapper (NFS portmap)	Application Servers
2049	TCP/UDP	Inbound	Disabled	NFS (nfsd)	Application Servers
2050	TCP/UDP	Inbound	Disabled	Mount Daemon (NFS mountd)	Application Servers
2051	TCP/UDP	Inbound	Disabled	Lock Daemon (NFS lockd)	Application Servers
2052	TCP/UDP	Inbound	Disabled	Stat Daemon (NFS statd)	Application Servers
Deprecated					
5747	TCP	Inbound	Disabled	HCP replication (deprecated)	HCP
10000	TCP	Inbound	Disabled	NDMP (deprecated)	Backup Servers

3.2.3 Transport Layer Security

Hitachi Vantara recommends using secure transports when transmitting data across the network. HCP uses the Transport Layer Security protocol (TLS 1.2) to ensure privacy and data integrity between the HCP and other systems with which it communicates. TLS is the successor to the Secure Sockets Layer (SSL) cryptographic protocol. TLS provides data in-flight encryption (DIFE) utilizing HTTPS for HCP services including HCP system management console, tenant management console, search consoles, RESTful API gateways, namespace browser, and cloud tiering. Replication is also performed securely and will be described in a following subsection.

TLS is configured at the HCP cluster level. This service allows you to set the minimum security protocol supported for front-end communications. The options are TLSv1, TLSv1.1 and TLSv1.2. The recommended minimum security protocol is TLSv1.2. However, HCP can electively enable TLS v1.0 or v1.1 to accommodate older browsers and applications; however, these older versions could increase the vulnerability footprint of HCP.

Once the TLS connection is established, the default behavior is that a Triple Data Encryption Standard (3DES) session key is generated for that specific connection and all data transmitted or received is encrypted or decrypted with this session key.

3.2.3.1 Server Authentication Certificates

For HTTPS communication, HCP maintains a server certificate utilized by the web service. This server certificate initially is a Secure Hash Algorithm 2 (SHA-2) self-signed certificate and generated at installation time. Organizations can also generate a new self-signed certificate to replace the one generated at install time to either update the details and/or replace an expired certificate.

To establish a trusted connection between the HCP client and the HCP server, the administrator should obtain a X.509 signed certificate from a known Certificate Authority (CA). To accomplish this, the HCP administrator generates a Certificate Signing Request (CSR) via the HCP administration console and provides the CSR to the CA. The CA will generate a signed certificate that is then be loaded into HCP.

Once this is completed, all clients connecting to the HCP will be able to trust the TLS connection and feel confident a man-in-the-middle attack is not possible.

3.2.3.2 Secure Replication

Replication communication is accomplished over a secure Transmission Control Protocol/Internet Protocol (TCP/IP) connection between the source and target systems. To establish a trusted TLS connection, the administrator must share a valid HCP server certificate with the other HCP server to be linked together. During the TLS TCP/IP establishment, the certificates are used to ensure the peer is a trusted HCP server.

Data transmitted over the network is encrypted using the highest common TLS version between the two servers as determined during its initial connection negotiation. The current versions supported are TLS 1.2, 1.1, and 1.0. The public key of the peer HCP system is used to encrypt the data when transmitting over the network.

3.2.4 Data Access Methods

HCP supports several industry-standard data access methods that include Amazon S3, Swift, WebDAV, Common Internet File System (CIFS), Network File System (NFS) and SMTP, as well as a proprietary REST application programming interface (API). They support both authenticated and anonymous types of access. When applications write an object, HCP conceptually puts it in a namespace/bucket along with associated metadata that describes the data. Although HCP is designed for “write-once, read-many” (WORM) access of information, namespaces can be enabled with versioning to permit write and rewrite input/output (I/O) semantics.

When a namespace is created, the only data access method enabled by default is authenticated HTTPS for the proprietary REST API. Any IP ports not in use by a disabled protocol are closed by the HCP firewall.

The following subsections visit each data access method in more detail and provide recommended secure approaches.

3.2.4.1 Cloud Optimized RESTful APIs (Ports 80/443)

The HCP REST API, Hitachi API for Amazon S3 API, and HCP Swift API provide namespace access through HTTP (port 80) and/or HTTPS (port 443) and are described as HCP’s RESTful APIs. Enabling a namespace’s “Cloud Optimized” property limits data access to only RESTful APIs. When the property is enabled, objects can be interchangeably ingested or read with any RESTful API, while other data access methods are permanently disabled. When all of the namespaces are cloud optimized, HCP has a smaller attack surface because it will not run any of the services associated with SMTP, WebDAV, NFS or CIFS, and will block all ports associated with these services in its firewall.

When Cloud Optimized is not enabled, non-REST access (discussed below) can also be utilized for ingest or read. Non-REST protocols include SMTP, WebDAV, CIFS, and NFS.

Hitachi Vantara recommends using only Cloud Optimized namespaces, if possible, establishing IP allow/deny lists, and only the HTTPS protocol enabled for those that are needed.

3.2.4.2 SMTP (IP Port 25)

Simple Mail Transfer Protocol (SMTP) can be enabled on any namespace that is not designated as Cloud Optimized. The SMTP service implements the SMTP protocol to ingest cleartext email directly into a namespace. This allows an HCP system to automatically archive email messages as they pass through one or more enterprise mail transport agents such as Microsoft Exchange or Sendmail.

Due to SMTP’s relative lack of security, IP address restriction of the protocol to specific clients is highly recommended using the allow or deny list. In general, individual users should not be given direct access to this interface.

3.2.4.3 WebDAV (IP Ports 80/443)

The WebDAV service provides web-based (HTTP) transfer of data to and from the namespace. HCP supports HTTP version 1.1 and WebDAV level 2 operations, and all traffic can be encrypted using TLS (HTTPS). Because WebDAV is unauthenticated, organizations planning to develop

new HTTP applications to access the object store are urged to code to RESTful APIs that provide namespace authentication.

3.2.4.4 CIFS (IP Ports 137, 138, 139, 445)

Microsoft Common Internet File System (CIFS) allows Microsoft Windows-based applications to interact with a namespace. The default tenant administrator can choose from two types of CIFS authentication: anonymous or Microsoft Active Directory (AD).

The **anonymous mode** does not perform any kind of user authentication and is not recommended.

Microsoft AD authentication will use Kerberos authentication via an Active Directory server to authenticate the users and allow a CIFS share to be mounted only by valid users. Use of Active Directory for authentication purposes is strongly encouraged to minimize administration and maximize security.

Objects ingested through the CIFS mounts have their Windows permissions mapped to Portable Operating System Interface (POSIX) attributes for cross-protocol compatibility. The HCP CIFS implementation does not support Windows ACLs.

3.2.4.5 NFS (IP Ports 111, 2049)

The Network File System (NFS) service in HCP implements NFS version 3, generally used with UNIX-based clients. When a client in the organization's environment mounts an NFS file system from the namespace, POSIX permission checking on the mount point is performed. Because the underlying operating system of the repository is Linux-based, POSIX-style permissions are natively enforced across all directories and files. As a result, access is restricted properly across user IDs and group IDs. Hitachi Vantara recommends restricting NFS access to namespaces to specific client IP addresses and limiting access to the mount command on those clients.

3.2.5 Network Services

HCP has a number of network services that provide object storage capabilities and management. These services operate over specific network ports and each should be considered as to the relevance for the HCP deployment and feature availability.

Enabling or disabling any of these services will result in the HCP hosted firewall to be changed to no longer allow connections over the relevant IP port. For more on firewalls, see Section ***3.2.2 Firewall Configuration***.

3.2.5.1 ICMP ECHO (ping)

By default, Internet Control Message Protocol (ICMP) echo (ping) response is **enabled**. Although these replies can be disabled on the network security page of the system management console, it is not generally recommended unless nodes are in the organization's demilitarized zone (DMZ) or perimeter network. Ping is arguably the most-used troubleshooting tool, so blocking ping traffic inside your network may make debugging unnecessarily harder.

3.2.5.2 HTTP/HTTPS Data Access (IP ports 80/443)

The HTTP/HTTPS communication is for data access by applications. HTTPS is **enabled** by default in a per namespace basis and the recommended protocol for tenant data access for all applications utilizing REST APIs.

By default, the HTTP protocol for data access is **disabled**; it is not recommended for applications utilizing REST APIs because all transmissions occur in cleartext. It can be enabled on a per namespace basis through the tenant management console, but that approach is not generally recommended except for development or debugging purposes.

3.2.5.3 NTP (IP Port 110)

Network Time Protocol (NTP) is a key component to ensure that HCP system time is correct. It is required for many security aspects, such as utilizing Microsoft AD.

Most HCP deployments operate with NTP **enabled**. HCP offers four time-server configurations:

- External time server – supply IP for one or more corporate time servers (NTP).
- Internal time server – time set by user, user adjustable.
- External time server – compliance mode, not user adjustable, IP provided at install for all NTP servers.
- Internal time server – compliance mode, not user adjustable, current time set at install.

NTP traffic occurs when HCP is configured with an external time server or servers. In this mode, HCP determines system time using NTP server or servers specified by the systems administrator. When installed as a compliant time system, administrators are prevented from adjusting or modifying time configuration after installation.

External time servers connected to HCP should be secure and trusted servers that are updated to NTP 4.2.8 or greater. Having multiple time servers can also help. A time server should never suddenly jump forward. If a time server does suddenly jump forward, NTP will interpret this event as a broken timeserver (a "false ticker") and exclude it from calculations until it is fixed. If the various NTP algorithms do conclude that the remote clocks are right and the HCP node is wrong (say, if *all* the remote timeservers agree, but the node still disagrees), and the offset is more than 1000 seconds (~16 minutes), then the node will reboot (realizing that it cannot reconcile its internal clock with outside evidence). This will force the clock to the "right" value on startup.

In the unlikely event that all NTP servers become compromised, you run the risk of violating compliance. For this reason, HCP does offer a closed system internal time server option. With an internal time-server installation, HCP timekeeping occurs in a closed system, and thus its nodes cannot be spoofed via a compromised NTP server or servers.

3.2.5.4 DNS (IP Port 53)

Domain Name Service (DNS) communication in HCP is utilized for both inbound and outbound communication. On inbound, HCP can act as an authoritative server for the HCP subzone. On outbound, HCP may require external DNS server to resolve needed host names for things like NTP, external storage systems, AD servers, etc.

By default, the inbound DNS protocol is **enabled**. It can be disabled on the configuration page of the system management console if using load balancers. HCP supports up to 32 downstream DNS servers, which is ample for most organizations. Other key capabilities include the HCP shadow (hidden) master, which allows authoritative DNS responses from servers purposely omitted from publicly visible Name Server (NS) records. The default behavior permits any host to receive the full zone transfer for a domain. Some organizations consider this a security issue since DNS data can be used to decipher the topology of a company's network. The information obtained can then be used for malicious exploitation such as DNS poisoning or spoofing.

An industry-standard way of preventing unauthorized zone transfers is to use DNS transaction signatures (TSIGs). A DNS TSIG provides a level of security that ensures information from the primary name server is authentic. It employs shared secrets and a one-way hash function to authenticate DNS messages, particularly responses and updates. HCP provides an advanced DNS configuration capability that includes support for TSIG, which is enabled via Management API (MAPI) command requests.

3.2.5.5 SSH (IP Port 22)

Secure Shell (SSH) console access is used by Hitachi Vantara customer service or authorized service providers to execute service procedures and diagnose system problems.

By default, SSH console access is **disabled** and should remain so unless specifically needed. This can be changed on the network security page of the system management console if the HCP system requires service. Hitachi Vantara service personnel can access the system using SSH2 strong authentication with password-protected, 2048-bit RSA authentication keys. While many vendors reuse the same key or password across different versions of the product throughout its life cycle, Hitachi changes security keys for every major software release.

Service users logging in over SSH2 will log in as the service user. This user does not have general root access to the system but does have sudo privileges for a subset of storage-related operations.

3.2.5.6 SNMP (IP Ports 161/162)

Simple Network Management Protocol (SMTP) is a protocol for different devices to share information with one another. By default, SNMP protocol is **disabled**. It can be enabled on the system management console along with settings for SNMP trap configuration and explicit control to pass or withhold compliance or security-related events. SNMP configuration is done at the system management console by a user with either the administrator or security role.

HCP can also be configured to allow remote management from an SNMP-based management application. Where the management server is running SNMP 1 or 2c, remote managers must share a community string with the system. If the management server is running SNMP 3, the remote manager must share a community string with the system and must authenticate with a username and password.

Once enabled, access to HCP via SNMP can be restricted by IP address using allow or deny lists. In addition, allowing remote management can be disabled.

3.2.5.7 Remote Syslog (IP Port 514)

Syslog is a standard for message logging. HCP allows configuration of sending system events via syslog to remote systems. By default, syslog service is disabled. This can be changed on the monitoring page of the system management console. Syslog can stream HCP event messages to one or more servers performing security audit functions. Users with administration or security roles can individually include/exclude the following message types:

- Log errors
- Log errors and warnings
- Log errors, warnings, and notifications
- Compliance events
- Security events (example logins)
- Management API activity
- HTTP access-log activity

Tenant administrators can use the tenant management console to opt in for remote logging of tenant-specific events. Configure this feature carefully to ensure that HCP is logging to the correct destination.

3.2.5.8 Hitachi Device Manager (IP Port 2001)

Hitachi Device Manager (HDvM) is a management framework with the primary focus of managing multiple Hitachi storage products from a single console. HCP can integrate with HDvM to send device information. By default, connection to Hitachi Device Manager (HDvM) is **disabled**. It is opened by enabling scheduled updates to HDvM in the system management console.

3.2.5.9 OpenStack Keystone (IP Port 5000)

OpenStack Keystone is an identity service that supports token-based authorization for the Hitachi Swift compatible protocol. By default, connection to OpenStack Keystone is **disabled**. It is opened by enabling OpenStack Identity Service in the system management console.

3.2.5.10 Replication Links (IP Ports 5747, 5748)

HCP offers replication capabilities for disaster recovery and global data access. Port 5748, **enabled** by default, is used to establish secure links between one or more HCP clusters and used to make data copies. Multiple links can be established between HCP clusters. Replication link communications are protected with TLS and secured using public key infrastructure (PKI). PKI authentication allows each HCP site to mutually validate the identity of its communicating partner. After authentication, HCP systems employ a proprietary communication protocol to conduct data replication. Replication data is not accepted until the replication request is accepted in the system management console.

Port 5747 is used to establish replication links with legacy deployments that have a different security standard, and is **disabled** by default. To enable port 5747, you must enable backward compatibility for replication in the system management console.

3.2.5.11 Management Consoles (IP Port 8000)

The system management console (SMC) and tenant management console (TMC) web interfaces are accessed via HTTPS over TLS at port 8000 on any storage node in the system and are **enabled** by default. There is a single administrator URL for the system management console. In

addition, each defined tenant has a distinct tenant management console URL. For example, if the URL of your HCP system is hcp-ma.example.com, the SMC would be accessed at **https://admin.hcp-ma.example.com:8000**. Continuing the example, the TMC for tenant "tenant-1" would be accessed at **https://tenant-1.hcp-ma.example.com:8000**.

3.2.5.12 Search Console (IP Port 8888)

HCP provides a search capability that is accessed via HTTPS through a system search console or tenant search console, which are both **disabled** by default. The web interfaces are accessed over TLS at port 8888 on any storage node on the system.

Only system-level users with search roles have access to the system search console. These users may only search tenants and namespaces that have search enabled – where the tenant administrator has granted the system user search capabilities. This prevents tenant data from being exposed in search results without the express permission of the tenant-level administrator.

Tenant users with the search role have access to the tenant search console. Such users may only search within the tenant in which that user is defined. Tenant users may only search namespaces where the tenant administrator has granted the user the search permission in the namespace's data access permissions.

There is a single URL for the system search console. For example, if the URL of your HCP system is hcp-ma.example.com, the system search console would be accessed at **https://search.hcp-ma.example.com:8888**. Continuing the example, the tenant search console for tenant "tenant-1" would be accessed at **https://tenant-1.hcp-ma.example.com:8888**.

3.2.5.13 Management API (IP Port 9000)

The Management API (MAPI) is a RESTful based interface that allows for querying and configuring most aspects of the HCP system. By default, the management is **disabled**. It is opened by enabling MAPI for the system. Authorization is granted by the system administrator using Role-Based Access Controls.

3.2.5.14 Node Status API (IP Ports 80/443)

The Node Status API provides a lightweight REST-based unauthenticated query-response mechanism that can be used by load balancers or diagnostic tools to poll node health. It shares the same port as the RESTful Data Access APIs; However, the response to the URL is **disabled** by default.

3.2.6 Private Virtual LAN (PVLAN)

Private Virtual LAN (PVLAN) (a.k.a. port isolation) is a networking technique where a VLAN contains switch ports that are restricted such that they can only communicate to other networks via a specific "uplink." By default, PVLAN support is **disabled** for HCP ports connecting to the front-end network ports because very few organizations deploy with this option. PVLAN is an isolation technique that is sometimes enabled on the organization's front-end switches. PVLAN ports block all traffic to anything but the "gateway" (switch or router) on the network segment, ensuring a compromised server cannot directly attack other servers on the subnet. PVLAN support can be enabled on request by Hitachi Vantara service personnel.

3.2.7 Miscellaneous Networking Configuration

There are a few additional miscellaneous networking configurations that are of interest to system hardening. These settings are available in the HCP System Management UI under *Security -> Network Security*. These are briefly mentioned in the table below for awareness for potential consideration.

Table 2. Miscellaneous Network Configurations for Hardening

Topic	Description
3DES Ciphers	Enables Triple-DES (3DES) ciphers for data encryption for HTTPS communication. While this is a secure cipher, some industries and government organizations may require the use of AES ciphers. Disable this feature to only allow AES ciphers to be used for encryption.
SSL Renegotiation	Enabling SSL renegotiation allows network connection to renegotiate the SSL/TLS process to change the details of the connection. With this feature enabled, there is the potential for a man-in-the-middle attack. Applications integrated with HCP typically do not require renegotiation and it is recommended to disable this feature.
SMBv1 Data Access Prevention	Server Message Block (SMB) version 1 contains many well-known security flaws. The largest is the lack of encryption, thus an attacker can obtain credentials and perform man-in-the-middle attacks. To disallow HCP clients from using this protocol, enable this feature.

3.3 Authentication and Access Controls

HCP has very robust and flexible capabilities for user authentication and access control. As a core concept, HCP allows multi-tenancy and namespace isolation. These features provide the ability to treat one installation of HCP as separate virtual HCPs providing separate management as well as ability to organize and protect different types of data into namespace(s).

Along with this, there is robust user authentication utilizing both local and standard authentication frameworks like Active Directory. And finally, access control to content can be controlled in multiple ways.

The following subsections outlines these key security features.

3.3.1 Multitenancy and Namespace Isolation

HCP is designed with strong multitenancy management, delegation, and provisioning features, separating management and data between departments or clients, limiting risk and confining exposure.

A single **HCP system** is the overall structure for managing one or more tenants. The HCP system enforces boundaries that keep the applications, users, and data of each tenant isolated.

Tenants provide management and control isolation at an organizational level but are bounded by policies set forth at the system-wide level. Each tenant is a virtual object storage system with independent management and data access, despite running on the same HCP instance. An HCP system can have many tenants. Each tenant hosts one or more namespaces: Each segregates data belonging to different applications and user communities.

A **namespace** is the smallest unit of HCP capacity partitioning, and it must follow policies set at the tenant level. Namespaces provide the mechanism for separating the data stored by different applications, business units or customers. Objects stored in one namespace are not visible in any other namespace. Namespaces provide segregation of data, while a tenant provides segregation of management.

3.3.1.1 Role-Based Access Control

The HCP system isolates the administration of the repository at the system level from the administration of individual tenants, and it isolates the administration of tenants and namespaces from access to the data in the namespaces (see ***Figure 2***). HCP provides role-based access controls (RBAC) for administrative accounts at both the system and tenant levels. The roles are System Administration, Compliance, Security, Monitoring, Search, and Service. An HCP administrator may fulfill one or more roles at the system and tenant levels. There is no single super user account in HCP. The boundaries between various administrative and data access domains limit the scope of damage that can be done by a malicious user through a compromised account.

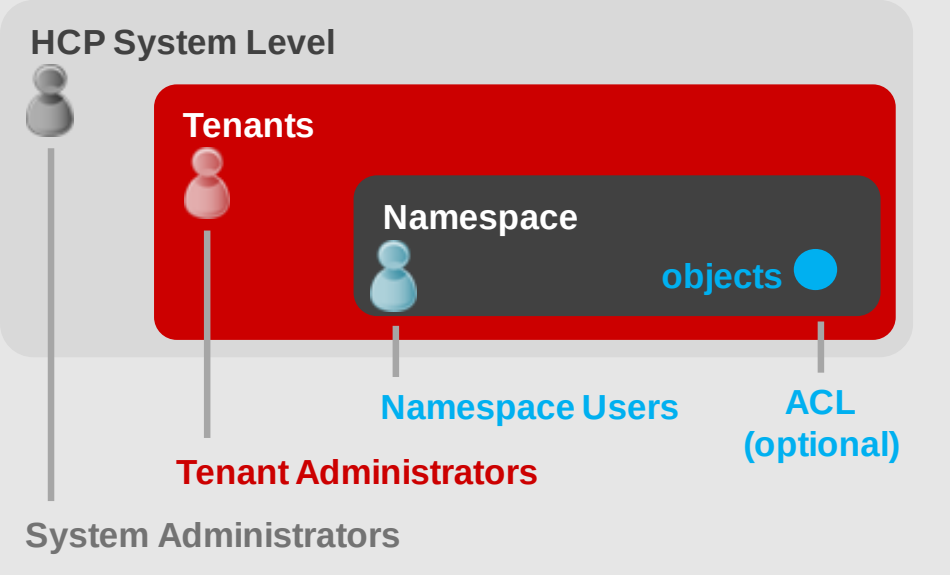

Figure 2. HCP Isolates Administration Levels

Users with system-level roles do not have further tenant-level access without an explicit action on the part of the tenant administrator. Tenant-level roles are explicitly associated with a set of one or more tenants and do not have access to other tenants.

The HCP system isolates system-level and tenant-level administration (see ***Figure 2***). Only **system-level** users have access to the **system management console (SMC)**. Once a system-level user with the administrator role creates a tenant, that administrator has no further tenant-level access without an explicit action on the part of the tenant administrator. Note that the system-level administrator role can reset the passwords of tenant-level users that have the security role. System-level users with administration roles cannot read or write data, but they do control how physical storage resources are virtualized and monitored. They design service plans to govern data placement, how it ages, and how it is retired. These managers prioritize system services, create tenants and delegate control over capacity using a quota system.

The HCP system further isolates administration of each tenant by providing each tenant with a private **tenant management console (TMC)**. There is a separate administrator URL for each defined tenant. While the TMC allows a tenant administrator to monitor, configure and manage the tenant and its namespaces, access to the data or listing the contents of any namespace requires explicit data-access permissions. Tenant administrators without explicit data access permissions cannot access data in a namespace. Note that the tenant-level administrator role can assign data access permissions to any user, including themselves.

Tenant administrators create and manage namespaces for application use at a micro level. They control namespace capacity through quotas and define user membership, access protocols, and service policies. They further define which users can read, write, delete, or search a namespace. The HCP system-level administrator controls the number of namespaces each HCP tenant can create.

Table 3. System-Level and Tenant-Level Administration

Scope	Available Administrator Roles	Login Access (Port)
System	Security, Monitor, Administrator, Compliance, Search, Service	System Management Console (8000) Search Console (8888) Management API (9090)
Tenant	Security, Monitor, Administrator, Compliance, Search	Tenant Management Console (8000) Management API (9090)

NOTE: ***Table 5*** in Appendix A describes the administrative roles (Security, Monitor, Administrator, Compliance, Service, and Search).

3.3.2 User Authentication

HCP utilizes user accounts and group membership to control access to the data, management consoles, APIs, and search console. New user accounts can be configured to authenticate locally or remotely, however, the authentication method for an existing user account cannot be changed. HCP validates users with any of the following authentication methods:

- Local authentication
- Remote Active Directory
- Remote Radius
- Remote Keystone (OpenStack Identity Service)

HCP allows remotely authenticated users to be assigned administrative roles at either the system or tenant management level. As such, HCP management permissions can be fully managed within Active Directory (AD) by assigning AD users to AD groups with administrative roles in HCP. However, there must always be at least one local HCP system user account with the security role. This system security account allows recovery from a situation where the HCP becomes partitioned from the AD environment.

By default, newly created locally authenticated users are asked to change their password on first login. System or tenant administrators with access to either of the system or tenant management consoles may change their own password in either of these consoles. Data access users who do

not have access to these consoles may change their own password using the namespace browser with a namespace in which they have permissions.

Resetting the passwords of users other than oneself requires the security role. System or tenant level users with the security role can reset passwords via the web console or via management API. This latter method allows security management tools (example CyberArk) to automate password administration.

HCP web administration consoles offer the following protections to help prevent unauthorized access:

- Enforce minimum password length
- Force password changes after specified period (days)
- Disable user account after unsuccessful login attempts
- Disable old inactive accounts
- Logout idle users

3.3.2.1 Local

For local authentication, HCP internally checks the validity of the specified username and password.

- **System-level** users supply username and password to access the system or tenant management console.
- **Tenant-level** users supply username and password to access the tenant management console.
- **Namespace** users supply username and password to access the namespace browser. When accessing a namespace by RESTful API these users must include username and password credentials in the request. This is done with an authentication token calculated as follows:

  Authorization HCP = `base64(username):md5(password)`.
  HTTPS is required to protect the token from packet sniffing attacks. Every authenticated request for data access is subject to the effective permissions of the user as determined by performing a Boolean AND with the system, tenant, and namespace permissions masks and data access account permissions. A user's ability to read, write, delete purge, or search objects is blocked unless all governing entities in the chain enable explicit affirmative rights.

3.3.2.2 Active Directory

Active Directory (AD) is a Microsoft product that, among other features, provides user authentication services. You can configure HCP to support access by users authenticated by AD. With HCP configured this way, an authenticated AD user can use any HCP interface that requires authentication, such as the system management console, the search console, or the applicable data access protocols.

HCP permissions for AD users are configured by utilizing AD groups. HCP uses the AD group to identify what administrative roles and namespace access permissions for all users in the AD Group. When a user's credentials are supplied, the AD group roles and permissions configured in HCP are consulted to determine allowed operations. You can choose to enable secure communication between HCP and AD. In this case, HCP needs a copy of the certificate that

allows clients to connect securely to the Lightweight Directory Access Protocol (LDAP) server used by AD. You need to export this certificate from AD as a base-64-encoded X509 certificate and then upload it to HCP on the Active Directory page.

For secure communication with AD, HCP uses Microsoft NT (New Technology) LAN Manager v2 (NTLMv2) by default for new AD connections. You can specify that HCP should use NTLM instead.

For HCP to use AD for user authentication:

- HCP must be able to contact at least one DNS server that can resolve the AD domain name. Additionally, HCP must be able to do a reverse DNS lookup of the IP addresses that HCP uses to communicate with each domain controller in that domain. (That is, the DNS configuration must include pointer (PTR) records for all AD domain controller IP addresses that HCP uses to communicate with AD.)
- The AD time must be the within five minutes of the HCP system time. The recommended configuration is for HCP and AD to use the same time server.
- All the domains in the AD forest HCP uses for user authentication must minimally be at the Windows Server 2003 functional level.

3.3.2.3 Radius

A system-level user with the security role can configure HCP to remotely authenticate against one or more RADIUS servers. For RADIUS authentication of an HCP user account, the HCP system must have network access to one or more RADIUS servers. To enable HCP to communicate with RADIUS, each RADIUS server must have at least one IPv4 or IPv6 address that is routable from the [hcp_system] network.

Authentication via RADIUS server is limited to authenticating in the HCP system and tenant management consoles and determining administrative roles allowed for the user. Data access authentication is not allowed with RADIUS users.

3.3.2.4 Keystone

Keystone is an OpenStack identity service that supports token-based authorization. Keystone generates authentication tokens with a predetermined expiration timer that are used to identify users attempting to store and manage containers and objects.

When connecting to Keystone through HTTPS, Keystone provides a TLS certificate, which if not signed by a trusted authority must be manually accepted. Once you agree to trust the certificate, it is cached for each future connection attempt to the Keystone server. Alternatively, you can manually upload the Keystone TLS certificate from your local machine.

Keystone authentication is only utilized for data access using the OpenStack HSwift protocol.

3.3.3 Data Access Control

The HCP system isolates the administration of tenants and namespaces from access to the data in the namespaces. Namespace users are created within the context of a tenant and assigned namespace data-access rights (read, write and so forth). The tenant administrator controls which namespaces within the tenant are visible to each data-access user. A data-access user created

in one tenant cannot access data in any other tenant, nor access the system management or tenant management consoles.

Data access within the repository is done only in the context of a specific namespace. Every level of administrative control in the repository can apply data access restrictions. HCP does this using permission masks. Permission masks are applied at the system level, the tenant level, and the namespace level. In namespaces, each data access account has permissions associated with it.

HCP provides multiple layers of access control to the data. Control can be placed on overall data operations at multiple levels using masks, access protocols can be limited to IP address(es) through IP white/black listing, individual users/groups can be assigned permissions to namespace(s), and individual objects can be controlled via Access Control Lists (ACLs).

The following section outlines details about each concept.

Hitachi Vantara recommends that all permissions are set to least required to ensure proper data protection.

3.3.3.1 Permissions Masks

Data access permissions masks is a multi-layered approach at controlling overall data access without having to change permissions for all users. A permission mask consists of basic operations like read, write, etc. For a full list, see ***Table 6. Permissions Operation Descriptions*** in Appendix A.

A permission mask can be controlled at the system, tenant, and namespace levels:

- The system-level mask applies across all namespaces.
- The tenant-level mask is set for each tenant and applies to all namespaces in that tenant.
- The namespace-level mask is set for each namespace in a tenant, and only applies to the namespace.

The effective permissions for a tenant are the operations allowed by both the system-level and tenant-level permission masks. That is, to be in effect for a tenant, a permission must be included in the system-level permission mask and in the tenant-level permission mask.

The effective permissions for a namespace are the operations that are allowed by the masks at all three levels. That is, to be in effect for a namespace, a permission must be included in the system-level permission mask, the tenant-level permission mask, and the namespace-level permission mask.

Table 4 shows an example of the effective permissions for a namespace given a set of data access permission masks.

Table 4. Effective Permission Masking

Permission Mask	Permissions					
	Read	Write	Delete	Purge	Priv. Delete	Search
Systemwide permission mask	✓	✓	✓	✓		✓

Permission Mask	Permissions					
	Read	Write	Delete	Purge	Priv. Delete	Search
Tenant permission mask	✓	✓	✓	✓	✓	
Namespace permission mask	✓	✓	✓		✓	✓
Effective permission mask	✓	✓	✓			

A tenant initially has all permissions in its data access permission mask. When a namespace is created, it also has all permissions in its data access permission mask.

HCP system-level administrators can change the systemwide permission mask at any time. HCP tenant administrator can change the tenant and namespace permission masks at any time.

3.3.3.2 Whitelist/Blacklist

For each interface to HCP (both management and data), a whitelist/blacklist can be assigned to ensure another level of protection from attackers. For data access, the tenant-level administrator can restrict namespace access originating from specific IP address(es) using allow or deny lists. The restrictions apply only to the namespace and protocol for which they are defined. Entries can specify a specific IP address, a comma-separated list of IP addresses, or blocks of IP addresses using mask (192.168.100.197/255.255.255.0) or CIDR (192.168.100.197/24) notation. IP address restriction of protocols to specific clients is recommended.

3.3.3.3 User Permissions

The user data access is performed via enabled data APIs or protocols (REST, CIFS and so forth) or the namespace's web console. A tenant user or AD group is assigned permission to namespace(s). These user permissions are a superset of the data access permissions. When a user requests an operation against content in a namespace, the data access permissions masks and the user permission masks are combined to provide the least privilege allowed. That is, if the data permission masks only allow read, but the user is allowed read and write, the user ultimately will only have read access to the namespace content.

Table 6 in Appendix A lists the permission masks that control access.

3.3.3.4 Access Control Lists (ACLs)

An access control list (ACL) grants permissions to perform operations on an individual object to specified users or groups of users. ACLs can specify read, read ACL, write, write ACL, and delete permissions. ACLs must be written to the application by the owning application via the REST APIs.

Since the ACL is a grant-based ACL, if the user does not have access to the namespace, the ACL can be used to provide the level of configured access without providing permissions to the whole namespace for the desired operation.

3.4 Customer Service

In the event that Hitachi Vantara Customer Service or a third party support provider needs to perform data collection or perform service procedures, the two access methods are via Secured Shell (SSH) over the network or via a connection to an HCP host boot console.

When accessing via the HCP node boot console, access is very limited. There is one user, “Install,” that is configured to allow password-based login. The password for this account is set during the initial HCP installation. Once logged in, the Install user session is controlled by a menu-based interaction that is limited to basic installation/configuration steps. This does not allow for access to any user data or configuration.

For more advanced service procedures, SSH must be utilized. SSH access can be enabled or disabled via the HCP system management interface. When enabled, SSH is possible via the external facing network of HCP. To authenticate the user, SSL password protected private keys are required. Hitachi Vantara manages a set of keys that are to be used only by authorized service personnel. If a customer or third party service provider wants to have their own set of keys, a set can be assigned by Hitachi Vantara.

If SSH access is not enabled over the external HCP network, SSH access via the internal HCP network can be accomplished. For the service personnel to connect to the HCP, it will require them to be onsite or the virtualized network configured to allow the service personnel laptop to connect. This SSH connection also requires SSH password protected private keys to authenticate.

For every major release of HCP, new SSH private keys are generated, thus providing for a periodic changing of the keys.

For the most secure system, Hitachi Vantara recommends **disabling** SSH access via the HCP System Management UI and only enable it if required by Hitachi Vantara service personnel.

3.4.1 Command Line Interface

Everyday administration functions are graphical user interface (GUI) and API-driven, and do not have access to the command line via SSH. This ensures that organizations can more credibly prove regulatory compliance, auditing, and non-tampering. However, there are occasions that with the assistance of Hitachi Vantara service personnel, the command line must be utilized to perform service procedures and/or collect system data.

Gaining access to the command line is a cooperative activity between the customer and Hitachi Vantara service personnel. The HCP administrator will facilitate connectivity to the HCP system either locally or remote for the SSH protocol. The service personnel will provide the password protected SSH key and enter the key password for the HCP version being utilized. NOTE: The keys for SSH access are changed every major release of HCP.

To perform service procedures, Hitachi Vantara support uses encapsulated menus and/or validated HCP commands to make changes. After the changes are complete the organization would disable access for customer support.

4. Malware

HCP is not suspectable to malware as it does not provide an execution environment for objects that are uploaded to it. HCP's primary function is to protect an object in its custody without bias, just like Amazon or any other object service. Client applications may write an *.exe or similar with a virus, and HCP dutifully stores it. HCP will protect and return objects to a client exactly as it was stored. Since the object is never opened or executed on HCP servers, it is immune. In short, the client is responsible for scanning such objects prior to ingestion or after retrieval.

To further protect against malware, HCP has the ability to protect against malware since the data stored is immutable due to HCP storage concept is Write-One-Read-Many (WORM); thus, any content written cannot be modified.

To protect against content removal, HCP namespaces can be configured to restrict deletion of objects through system, tenant, and namespace permission masks, account permissions, and namespace policies. Permission masks allow the administrator to set an overall access permission like deny delete capabilities at the various levels regardless of what the individual user account is assigned for permissions. Namespace policies allow for setting time-based retention of objects that does not allow objects to be removed until the set time has been reached.

HCP also has the feature to allow for object versioning. Since objects in HCP store with WORM semantics, objects are immutable; however, with versioning it allows for writing an object with the same name, but the older versions will be maintained for the configured amount of time. In the event of a malware attach, older object versions prior to the attach can be retrieved to effectively restore the uninfected objects.

Before adjusting any of the topics mentioned in this section, make sure that the application integrated with HCP can properly operate with the configuration. For instance, if the application requires the ability to delete content, this should not be configured on HCP for the application environment.

5. Auditing and Monitoring

Consider making periodic reviews of HCP event logs. The system management console and the per-tenant tenant management consoles provide displays of critical system events. Users with accounts at these consoles will see different sets of events depending on the administrative roles assigned to their account. For example, security-sensitive audit records will not be visible to users that have not been granted the security role.

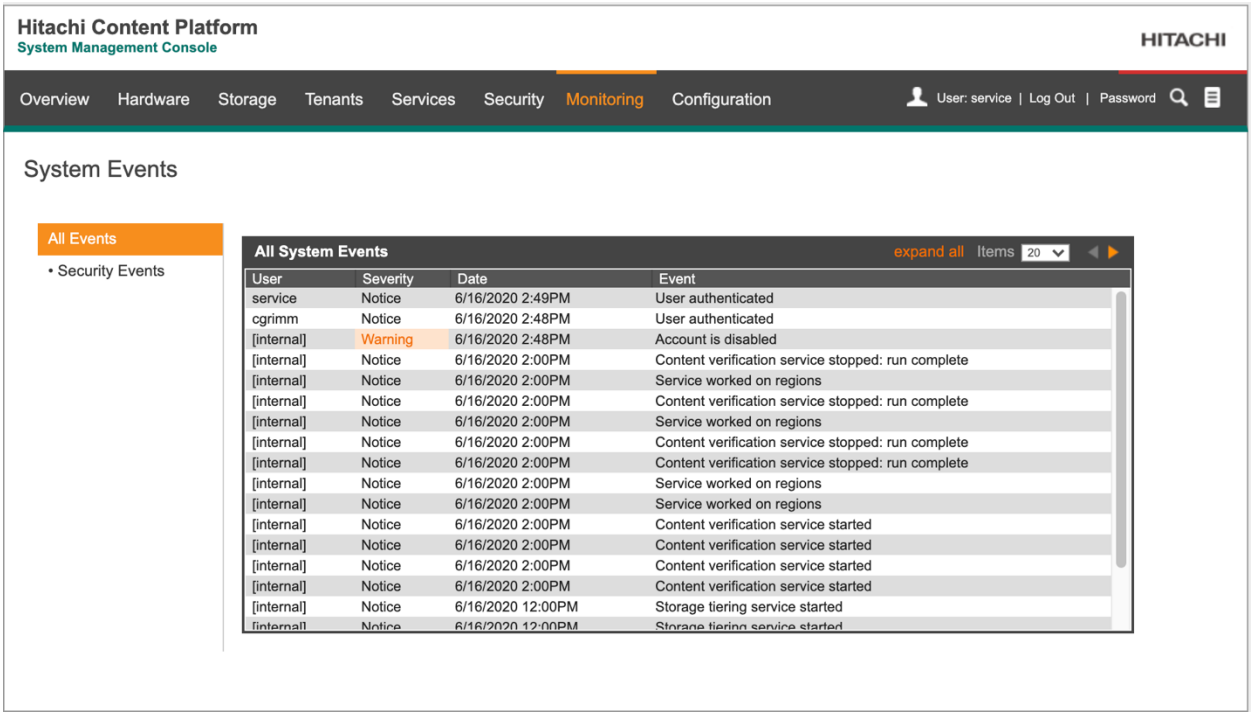

Figure 3. Monitoring and Logging of System Events

HCP event logging is quite extensive. Events of security interest to HCP administrators are listed in ***Appendix B: Events of Security Interest***.

6. Conclusion

Hitachi Content Platform has been designed with many security features to create a safe and secure repository of digital information. Through a combination of segregated namespace access for each application, access restriction by IP address, lockdown of all nonessential services, and unique directory structures for each application, HCP supports the easy construction of a large, multitenant repository that ensures that users cannot access data they should not be able to access. By following the recommendations in this whitepaper, organizations can build an enterprise-class repository infrastructure to support the needs of multiple applications.

7. Appendix A: HCP Administrator Role and Permission Description

Table 5. HCP Administration Descriptions

Role	Description
Security	A user with the *security* role has the ability to create and delete system management console user accounts and assign appropriate roles to them. Hitachi Vantara recommends that the number of accounts with this role be extremely limited.
Monitor	A user with the *monitor* role allows the user to view configuration settings and system status but not alter the system configuration.
Administrator	A user with the *administrator* role can view and modify the system configuration. Users with this role can create new tenants. They can also create the default tenant and namespace and use the Tenant Management Console for the default tenant to manage the default namespace access protocols and services. Hitachi Vantara recommends that the number of user accounts with this role be limited.
Compliance	A user with the *compliance* role has the ability to use the Tenant Management Console of the default tenant to view and modify data protection properties of the default tenant and namespace. This specifically includes retention, disposition, and shredding settings.
Service	A user with the *service* role has the ability to view additional system information not available to the other roles and to perform service procedures on the system. The service role is generally reserved for use by Hitachi Vantara authorized service personnel.
Search	A user with the *search* role has the ability to log into the HCP Search Console and perform queries across all data present in the default namespace if the HCP system includes the search facility.

Table 6. Permissions Operation Descriptions

Operation	Description
Read	Read and retrieve objects, including object metadata, and list directory contents.
Write	Add objects to a namespace, modify object metadata, and add or replace custom metadata.
Delete	Delete objects and custom metadata.
Purge	Delete all versions of a versioned object with a single operation. For users to perform purge operations, delete operations must also be allowed.
Privileged	Delete or purge objects under retention. For privileged delete operations, delete operations must also be allowed. For privileged purge operations, purge operations must also be allowed.
Search	Use the Search Console to search a namespace. For users to search a namespace, read operations must also be allowed.
Change Owner	Ability to assign an owner to the namespace (or bucket).
Read ACL	Ability to read the Access Control List (ACL) assigned to an object in a namespace.
Write ACL	Ability to write an ACL to an object in a namespace.

8. Appendix B: Events of Security Interest

System-level Events

- Changes to the configuration of any service
- OpenPGP key uploads or deletes
- Replication TLS certificate uploads or downloads
- Administrative user account creation, update, or deletion
- Administrative user authentication errors
- Administrative user login errors, differentiated by unknown username or invalid password
- Attempts to perform operations beyond assigned administrative roles
- Changes to remote (RADIUS) authentication configuration
- Remote authentication errors
- Password changes
- Accounts enabled and disabled or disabled due to excessive authentication errors
- TLS certificate upload or generation or CSR generation
- NDMP signing or encryption key uploads or deletes
- Network Service started/stopped/enabled/disabled
- Tenant creation or deletion

Tenant-level Events

- Namespace creation, update, or deletion
- Data access account creation, update, or deletion
- Data access account enabled or disabled
- Data access account password changes
- Data access failed login or attempt to login on a disabled account
- Tenant administrative user account creation, update, or deletion
- Tenant administrative user authentication errors
- Tenant administrative user login errors, differentiated by unknown username or invalid password
- Tenant administrative account password changes
- Tenant administrative accounts enabled and disabled or disabled due to excessive authentication errors
- Remote administrative authentication errors