WHITE PAPER

Hitachi Content Platform (HCP)

An Overview of Server Security and Protection

By Hitachi Vantara

October 2017

Contents

Executive Summary

This paper focuses on the various security features built into Hitachi Content Platform (HCP) cloud storage software to protect data access and secure communications. These features are designed to help administrators and network engineers establish a set of best practices for product deployment that minimize vulnerability 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 software includes layers of security, including physical, network, tenant, administration and data access. Other security features include use of certificates, data-in-flight encryption (DIFE), IP whitelisting and blacklisting, data-at-rest encryption (DARE) and regular security scans.

The system enforces multitenancy and namespace isolation to create virtual object stores that maintain separation between applications, users, data and storage.

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 independently set at the system level or tenant level. Administrators have constrained access to functionality, based on their role and scope.

Data Access Isolation: Data access is controlled by ACLs in which the most restraining permission is enforced to avoid oversharing. 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 AES-256 block cipher with a key (or block) length of 256 bits. This is the cipher required for 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, 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 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 VLANs or physically separate Ethernet ports available on HCP servers.

Introduction

Hitachi Content Platform 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.

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.

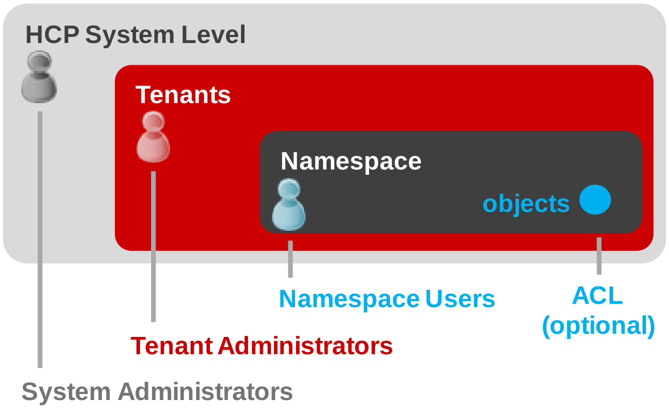
Tenants provide management and control isolation at an organizational level, but are bounded by policies set forth at the system-wide level. Each tenant is a virtual object storage system with independent management and data access, despite running on the same HCP instance. An HCP system can have many 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.

Role-Based Access Control for Management

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 1). 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 1. 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 Table 1). 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, 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 1. 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)

The table in Appendix A describes the administrative roles (security, monitor, administrator, compliance, service, and search).

Data Access Control List Permissions

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 by the use of permission masks. Permission masks are applied at the system level, the tenant level and the namespace level. In namespaces other than the default namespace, each data access account has permissions associated with it.

At the time any operation is performed, the system-wide, tenant and namespace masks are ANDed together to form an effective permission mask. For access within an authenticated namespace, an effective permission mask is ANDed with the permissions specified in the data access account to determine if the operation is allowed.

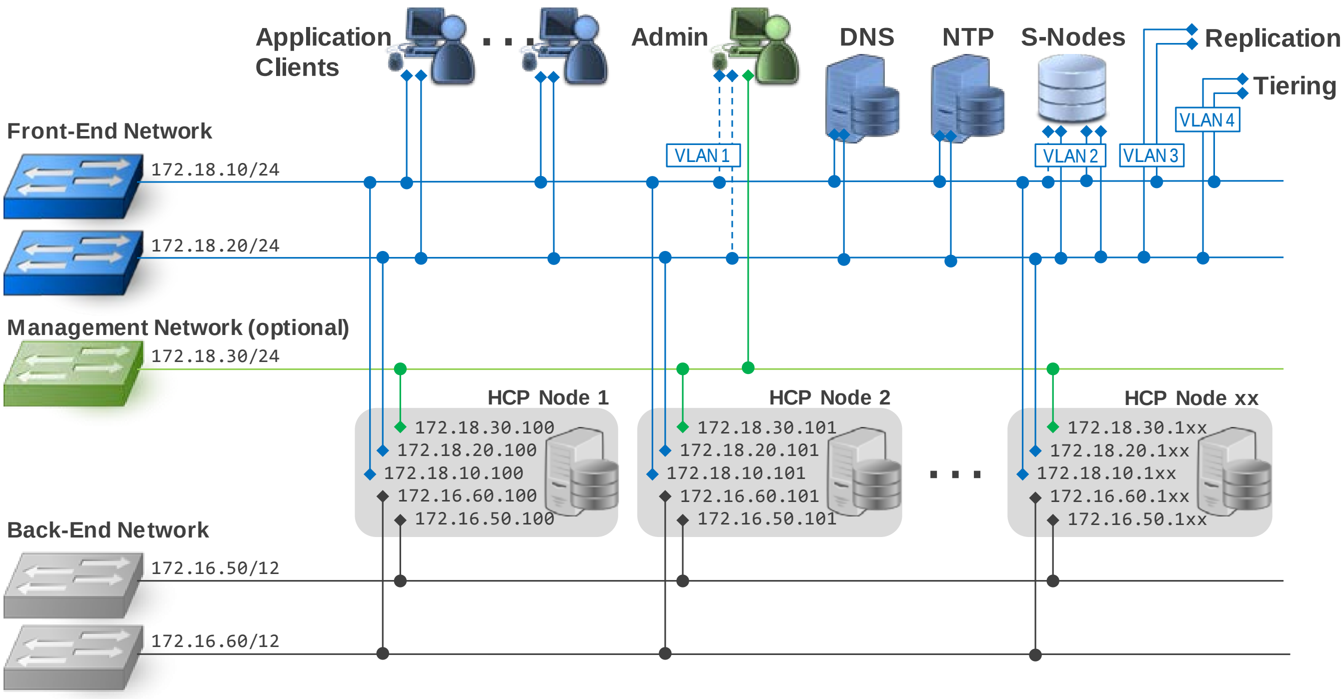
The data access is performed via enabled data APIs or protocols (REST, CIFS and so forth) or the namespace's Web Console (port 443).

The table in Appendix A lists the permission masks that control access.

Networking 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 2 provides a simple HCP network diagram.

Figure 2. Hitachi Content Platform Network Diagram



Private Back-End Network: Two switches along with all network cables are provided as part of an HCP appliance. These networks carry traffic vital to internode communication. It is presumed that these switches and ports are physically 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 nonroutable 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 physically separated from the data network. When initially installed, HCP administration activities occur on the front-end network with optional VLAN tagging, including *SSH, SMTP, Syslog, SNMP, MAPI* and *web consoles* for system, tenant and namespace management. HCP software v8.x can, instead, direct these management services to a (previously unused) physical 1Gb Ethernet port specific to HCP G10 servers, creating a physically 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 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.

Ports Potentially Used by HCP

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 2 presents a list of ports HCP might need during operation. The actual needs vary by specific deployment needs.

Table 2. 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
NFS 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

Transport Layer Security

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 for HCP services, including HCP system management console, tenant management console, search consoles, RESTful API gateways, namespace browser, replication and cloud tiering. By default, HCP uses TLS 1.2 for all communications. HCP ships with a default, SHA-2 self-signed certificate that can be used by organizations that do not wish to provide their own. Once the TLS connection is established, a 3DES session key is generated for that specific connection and all data transmitted or received is encrypted or decrypted with this session key. HCP allows organizations to upload multiple X.509 certificates to protect communications. The system management console can assist in generating a CSR for transmission to the organization's preferred signing authority. HCP can also generate and install a new self-signed certificate when a self-generated certificate expires (five years). Hitachi Vantara recommends the use of HTTPS for all HTTP data access. HCP can electively enable TLS v1.0 or v1.1 to accommodate older browsers and applications, but the organization should be conscious of known vulnerabilities.

Detailed Network Security Considerations

Hitachi Content Platform software also operates its own internal firewall, and many ports can be disabled via HCP administration actions as explained below.

Virtual Private LANs (PVLAN)

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.

Port 7 ICMP ECHO (ping)

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

Port 22 SSH Access

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.

Port 53 DNS Service

By default, 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 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 TSIG (transaction signatures). 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 advance DNS configuration capability that includes support for TSIG, which is enabled via MAPI command requests.

Port 80 HTTP Service for Tenant Data Access

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.

Port 123 NTP Service

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 of your 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.

Port 161, 162 SNMP Service

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. The format of these lists is the same as is supported for the system management console.

Port 443 HTTPS Service for Tenant Data Access

By default, HTTPS protocol for tenant data access is **enabled and recommended for** all applications utilizing REST APIs. It can be disabled on a per namespace basis through the tenant management console.

Port 514 Remote Syslog

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.

Port 2001 Hitachi Device Manager

By default, connection to Hitachi Device Manager (HDvM) is **disabled**. It is opened by enabling scheduled updates to HDvM in the system management console.

Port 5000 OpenStack Keystone

By default, connection to OpenStack Keystone is **disabled**. It is opened by enabling OpenStack Identity Service in the system management console.

Port 5747 Replication Links (deprecated)

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.

Port 5748 Replication Links

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 PKI (public key infrastructure). 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 8000 Management Consoles

The system management console and tenant management console web interfaces are accessed via HTTPS over TLS at port 8000 on any storage node in the system and **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**.

Port 8888 Search Console

HCP provides a search capability that is accessed via HTTPS through a system search console or tenant search console, which are **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**.

Port 9090 Management API

By default, the management is **disabled**. It is opened by enabling MAPI for the system.

Node Status API

Status API provides a lightweight REST-based unauthenticated query-response mechanism that can be used by load balances or diagnostic tools to poll node health. It is accessed on port 80 or port 443, and is **disabled** by default.

Data Access Methods

Hitachi Content Platform supports several industry-standard data access methods that include Amazon S3, Swift, WebDAV, CIFS, NFS and SMTP, as well as a proprietary REST API. They support both authenticated and anonymous types of access. When applications write a file, HCP conceptually puts it in a bucket (namespace) 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 I/O semantics.

By default, all data access services for the namespace are disabled: None of the daemons that provide these services are running, and the corresponding IP ports are closed by the HCP firewall.

Whitelist or Blacklist

The tenant-level administrator can restrict namespace access originating from specific IP addresses 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.

RESTful "Cloud Optimized" APIs: HCP REST, HS3, Swift

The HCP REST API, HS3 API, and SWIFT API provide namespace access through HTTP (port 80) 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, CIFS, NFS and WebDAV.

Port 25 SMTP Service

SMTP can be enabled on any namespace that is not designated as cloud optimized. The SMTP service implements the Simple Mail Transfer Protocol (SMTP) 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. And, in general, individual users should not be given direct access to this interface.

WebDAV Service

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 which provide by namespace authentication.

CIFS Service

The CIFS service implements the Microsoft Common Internet File System (CIFS), allowing 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.

The Microsoft Active Directory mode will use an Active Directory server to authenticate the users and allow a CIFS share to be mounted only by valid users. In Active Directory mode, HCP uses Kerberos authentication. 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 POSIX attributes for cross-protocol compatibility. The HCP CIFS implementation does not support Windows ACLs.

NFS Service

The NFS service implements Network File System (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 the namespace to specific client IP addresses and limiting access to the mount command on those clients.

Data-in-Flight Encryption (DIFE)

Hitachi Content Platform software offers TLS encryption to secure data passed to and from clients. The TLS enabled-services are compatible with TLS v1.2, v1.1 and v1.0.

HCP enables any of its supported data protocol that uses TCP to run over TLS connections. This includes cloud-optimized REST protocols, CIFS/Samba and NFS.

User Authentication

Hitachi Content Platform uses system-level user and group accounts 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 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 Active Directory environment.

By default, newly created 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.

Both system-level and tenant-level consoles offer tools that restrict access to specific IP addresses using allow or deny lists. Each list entry 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.

Local Authentication

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 ANDing 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.

Active Directory Authentication

Active Directory or 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.

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 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 Active Directory, HCP uses 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 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.

Radius Authentication

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.

Keystone Authentication

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's cached for each future connection attempt to the Keystone server. Alternatively, you can manually upload the Keystone TLS certificate from your local machine.

Auditing and Monitoring

Consider 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.

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

Limiting Command Line Interface (CLI) Risk

Even system administrators do not have command line access to Hitachi Content Platform systems so that organizations can more credibly prove regulatory compliance, auditing and nontampering. This approach comes with a security benefit as well because access to the system command line – even with restricted capabilities – both empowers an attacker to gain useful information or make secret changes, and increases risk of a legitimate user mistakenly causing data loss or system downtime.

Everyday administration capabilities are GUI- and API-driven, but there are rare changes that must utilize the command line. For these situations HCP's approach increases security by preventing clandestine manipulation: Making system changes that require command line access involves the cooperation of both the organization's administrator and authorized Hitachi Vantara customer support.

The process to modify the system requires the organization to enable access for Hitachi Vantara customer support; then Hitachi Vantara support must be authenticated for access; finally Hitachi Vantara support uses validated HCP commands to make changes. More specifically, the organization must open a support ticket with Hitachi Vantara, enable SSH access on HCP, open the SSH ports on appropriate firewalls, and provide access information for the Hitachi Vantara support representative. Hitachi Vantara support then uses a carefully controlled authentication key to access the HCP CLI as a support user, and may utilize a set of validated HCP CLI commands to make system changes. After the changes are complete the organization would disable access for customer support.

Virus Scanners

Hitachi Content Platform Anywhere (HCP Anywhere) servers can be configured to communicate to a corporate virus-scanning engine. But the HCP repository itself does not incorporate a virus scanner because HCP does not provide an execution environment for objects that are uploaded to it. HCP's job 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 it, and give it back to a client exactly as it was stored. Since the file is never opened or executed on HCP servers, it's immune. In short, the client is responsible for scanning such objects on deposit or retrieval.

Ransomware and Data Protection Strategies

Hitachi Content Platform offers several capabilities that protect data from data loss, including preventing or reversing a ransomware attack. (Ransomware is malware that encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.)

WORM

All information stored in an HCP system is “write once, read many” (WORM). With WORM mode activated, data written to the repository cannot be modified, and thus is immune to ransomware attacks. Depending on the configuration of the namespace in which the data resides, deletion of data from the namespace may be allowed.

Versioning

HCP supports the storage of multiple versions of an object. This feature can protect data from accidental deletion and can be used to roll back undesired or accidental changes. A system-level administrator can enable this feature for a tenant when the tenant is created. If this feature is enabled for a tenant, it can be enabled or disabled independently for each namespace within the tenant at any time. The tenant administrator can configure how long prior versions of each object are kept.

Retention

HCP provides flexible retention capabilities to prevent the accidental or malicious deletion of objects in the repository. Retention specifies the earliest time at which an object can be deleted.

HCP provides an option for infinite retention to require objects to be kept forever. It also provides a retention state of unspecified, which disables deletes for the object until the object has been assigned a retention value, after which standard retention rules apply. Objects that have no retention defined or have met their retention criteria and are now expired, are eligible for new retention criteria to be applied.

File Integrity: Prove Authenticity

A hash is computed for every object at ingest time to ensure data integrity. This “digital fingerprint” is stored as metadata and use to validate integrity of file upon retrieval. If there is any discrepancy or integrity breach, HCP automates object repair to fully restore the original data object from replica copies.

Tenant-level users (with admin role) can assign the cryptographic hash on per namespace basis. Available algorithms offered include MD5, SHA-1, **SHA-256 (default)**, SHA- 384 or SHA-512.

Hitachi Content Platform: System Hardening

The software was 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 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 SSL ciphers.
  - Form injection attacks.
  - Cross-site scripting (XSS) attacks.
  - Cross-site request forgery (CSRF) attacks.
- Passed Security Technical Implementation Guide (STIG).
  - Scan software used to validate server security conformance (DoD DISA).
- 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 for Common Vulnerabilities and Exposures (CVE).

https://knowledge.hitachivantara.com/Support_Information/CVE_Security_Notices/CVE_Index_Page

Conclusion

Hitachi Content Platform has been designed with many security features to create a safe, secure repository for long-term archiving 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 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 white paper, organizations can build an enterprise-class repository infrastructure to support the needs of multiple applications.

Appendix A: HCP Administrator Role and Permission Descriptions

Table 3. HCP Administrator 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. HDS 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. HDS 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 HDS 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 4. Permission 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	Applies to a namespace (or bucket). ■ View and change the versioning status of the namespace ■ Delete the namespace See the namespace in a namespace listing

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

Appendix C: Best Practice Security Deployment Summary

Physical security

- ☐ Limit physical HCP hardware access to a minimum set of trusted and qualified persons (lock rack/room)
- ☐ 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, firewall unused ports
- ☐ Disable SSH except during service periods
- ☐ Disable HTTP access except for debug
- ☐ Disable support for TLS1.0 and 1.1
- ☐ Establish multiple virtual (sub)-networks and/or utilize VLANs to logically segregate traffic types (E.g. Application, Tiering, Replication, Management)
- ☐ Ensure NTP and 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)

Server administration

- ☐ Keep HCP software updated to ensure latest bug fixes and CVE protections
- ☐ Mandate HTTPS is used for administrative functions and use allow/deny filtering of source IP addresses
- ☐ Utilize roles to segregate system administration responsibilities

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com | community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

WP-568-A T. Desai October 2017