



Hitachi Content Platform Layered Security Approach

Highly Scalable, Cloud-enabled Platform Ensures Data
Safety with Industry Standard Security Measures

By Hitachi Content Platform Engineering – Technology Team

December 2010

Table of Contents

| | |
|---|-----------|
| Executive Summary | 3 |
| Introduction | 4 |
| Summary | 4 |
| About Hitachi Content Platform Security | 4 |
| Authentication | 4 |
| Management User Interface | 4 |
| Data Access | 5 |
| Remote Authentication | 5 |
| Legacy Protocols | 5 |
| Console User | 6 |
| Remote Service Login | 6 |
| Internode Login | 6 |
| Authorization and Access | 6 |
| System Administration | 6 |
| Tenant Administration | 7 |
| Data Access Permissions | 8 |
| Authenticated Namespace Data Access | 9 |
| Default Namespace Data Access | 9 |
| Console Access | 10 |
| Service Access | 10 |
| Encryption | 10 |
| Data at Rest Encryption | 10 |
| Data Transmission Encryption | 10 |
| Auditing and Monitoring | 11 |
| Hitachi Content Platform Security Best Practices | 12 |
| Physical Security | 12 |
| System Management | 12 |
| Tenant Management | 12 |
| Service Management | 13 |
| Conclusion | 13 |

Executive Summary

Hitachi Content Platform (HCP) provides strong support for a full set of industry standard security measures. As a distributed object store, HCP is designed to provide a highly scalable, secure, cloud-enabled object repository platform capable of supporting multiple simultaneous applications. With layered security, the platform restricts unauthorized access to data to ensure its safety. This white paper summarizes the major areas of security in an HCP system and how they apply to object storage, access protocols, system administration and operation of the repository.

Introduction

Summary

Security is an important feature of your enterprise information infrastructure. Hitachi Content Platform provides multiple layers of features designed to safeguard and secure the data entrusted to it.

The primary purpose of this white paper is to address questions, such as:

- How does HCP prevent unauthorized management and configuration activity?
- How does HCP prevent unauthorized access to data?
- What options do I have for segmenting management and data access within HCP?
- What practices do I need to employ to minimize threats of unauthorized access?

About Hitachi Content Platform Security

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. HCP also includes several security features not found in other commercial object stores.

HCP supports multiple tenants: virtual object stores with independent management and data access. Each tenant can host multiple namespaces that segregate the data from different applications and user communities.

Authentication

Access to Hitachi Content Platform is segregated by user function. There are administrative accounts for managing the whole repository. Each tenant is granted a private set of administrative accounts. Tenant administrators establish data access accounts, which allow access to data within the namespaces of a tenant.

Management User Interface

The HCP Repository is managed at a browser-based System Management Console. Users of the System Management Console authenticate for access with a username and password. HCP is delivered with an initial management account with a default username and password. When this account is first used, the user is forced to change the password.

Tenants are created at the System Management Console. Once created, each tenant is managed at a browser-based Tenant Management Console. Users of each Tenant Management Console authenticate for access with a username and password. An initial administrative user account is created for each tenant when the tenant is created. The administrator who creates the tenant provides an initial password for this account. When the account is first used, the user is forced to change the password. Once changed, users of the System Management Console do not have access to the password or any of the tenant administrative accounts. The System Management

Console can, however, be used to reset certain tenant administrator passwords. The discussion of administrator roles later in this document talks more about this.

Data Access

Access to an HCP namespace to read or write data is done via HTTP. Tenant administrators grant access to namespaces within the tenant by creating data access accounts for the tenant and specifying the namespaces that each data access user can access. Each account has a username and password. Each HTTP request must present a cookie, which provides a valid data access account username and password.

Remote Authentication

By default, administrative accounts for the System Management Console and Tenant Management Consoles are authenticated against a locally managed username and password database. The System Management Console can be used to establish an external RADIUS server for use in authenticating HCP administrative accounts. Once an external RADIUS server is established, local or remote authentication can be selected on a per-user basis.

Legacy Protocols

The multitenant architecture in HCP is a recent feature. Earlier versions of HCP provided a single unified namespace, which was accessed by a number of standard Internet services. For compatibility with earlier versions of the product, HCP allows the system administrator to enable a tenant named *default* with a single namespace named *default*. Once this tenant and namespace are configured, users that can authenticate to the System Management Console can enable and disable access by way of specific network services. The sections that follow discuss how data access users authenticate to the individual services.

HTTP/WebDAV

A system administrator can use the Tenant Management Console for the default tenant to require WebDAV basic authentication for WebDAV transactions; otherwise, there is no authentication required for read and write access via HTTP or WebDAV.

CIFS

The HCP default namespace can be accessed by CIFS. The system administrator can choose to allow anonymous (unauthenticated) mount access or to configure authentication via an Active Directory server.

NFSv3

The default namespace can be accessed by NFSv3. NFSv3 does not provide an authentication mechanism.

SMTP

The default namespace can be used by a Mail Transport Agent to archive email over SMTP. The SMTP server does not need to authenticate with HCP to send email traffic.

NDMP

The default namespace can be accessed through NDMP for backup and restore operations. The NDMP interface can be configured to use username/password or digest authentication.

Console User

HCP does not support general console access to any of the servers that make up the system. It is not possible for a root- or super-user to authenticate at the console. There is one console per user account for system installation and upgrades. There is a default initial password for this account, which must be changed during the first login.

Remote Service Login

If a user at the System Management Console has authorized service access through ssh, a qualified HDS or Hitachi TrueNorth Channel Partner service team can use key-based authentication to access the service account on any of the HCP nodes.

Internode Login

HCP nodes are capable of performing a number of internode operations by way of ssh over the HCP back-end network. Key-based authentication is used to support this capability. The keys are not accessible to users of the HCP system.

Authorization and Access

System Administration

The System Management Console web interface is accessed at port 8000 on any storage node in the system. For example, if the name of your Hitachi Content Platform is `hcp-ma.example.com`, the System Management Console would be accessed at `https://hcp-ma.example.com:8000`. Administrators logging into this interface are authenticated with a username and password.

The HCP System Management Console uses role-based access controls (RBAC) for administrative accounts. The administrative roles are security, monitor, administrator, compliance, service and search. Table 1 describes these roles.

**TABLE 1. HCP SYSTEM MANAGEMENT CONSOLE
ROLE-BASED ACCESS CONTROLS**

| Role | Definition |
|---------------|---|
| 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 Data Systems 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 with an account for accessing the tenant-specific Tenant Management Console. They can also create the default tenant and namespace and manage the default namespace access protocols and services. Hitachi Data Systems recommends that the number of user accounts with this role be limited. |
| Compliance | A user with the compliance role has the ability 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 Data Systems 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. |

A system administrator with the security role can restrict the IP addresses that have access to the System Management Console using allow/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.

SSL encryption for access to the System Management Console is enabled by default using a self-signed certificate provided with the system. An **administrator** with the administrator role can upload new PKCS12 certificates. The System Management Console can also assist in generating a CSR for transmission to an administrator's choice of signing authority. HCP can also generate and install a new self-signed certificate when a certificate expires.

Tenant Administration

Each tenant has a private Tenant Management Console accessed at port 8000 of the tenant address. For example, if the administrator for the `hcp-ma.example.com` system created a tenant named `europa`, the tenant-level users for `europa` would access the Tenant Management Console as `https://europa.hcp-ma.example.com:8000`.

As with the System Management Console, HCP supports role-based access control for any number of administrative accounts within each tenant. Table 2 describes the tenant administrator roles.

**TABLE 2. HCP TENANT MANAGEMENT CONSOLE
ROLE-BASED ACCESS CONTROLS**

| Role | Definition |
|---------------|--|
| Security | A tenant administrator with the security role has the ability to create and delete Tenant Management Console user accounts and assign appropriate roles to those accounts. Hitachi Data Systems recommends that the number of tenant administrators with this role be extremely limited. |
| Monitor | A tenant administrator with the monitor role can view tenant and namespace configuration and status. They cannot change the configuration of the tenant or its namespaces. |
| Administrator | A tenant administrator with the administrator role can view and modify the configuration of the tenant and its namespaces. Users with this role can create namespaces and change namespace configuration settings. They can also create and modify data access accounts and specify the permissions for each account. Hitachi Data Systems recommends that the number of user accounts with this role be limited. |
| Compliance | A tenant administrator with the compliance role can view and modify data protection properties of each of the tenant's namespaces. This specifically includes retention, disposition and shredding settings. Users with the compliance role can also use the Tenant Management Console to perform privileged delete operations in namespaces in enterprise mode provided delete and privileged delete are enabled in the effective permissions mask for the namespace. |
| Search | There is no tenant-level search role. A tenant administrator with the security role can grant a system-level administrator with the search role access to use the search console to search content in the tenant's namespaces. |

A tenant administrator with the security role can restrict the IP addresses that have access to the Tenant Management Console using allow/deny lists. The list entry format is the same as for the System Management Console.

Data Access Permissions

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. Permissions 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. The permissions masks control access, as described in Table 3.

TABLE 3. HCP PERMISSIONS MASKS

| Role | Definition |
|-------------|--|
| 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. |

At the times 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, effective permissions mask is ANDed with the permissions specified in the data access account to determine if the operation is allowed.

Authenticated Namespace Data Access

Tenant administrators have very fine-grained control over access to data in each namespace within the tenant. In the Tenant Management Console, the tenant administrator creates data access accounts for the tenant and grants each account access rights to specific namespaces. Each tenant can have as many as 100 data access accounts. Data access accounts for one tenant are limited to that tenant.

Data access users are assigned a set of permissions. Combined with the permissions mask for the namespace, they are used determine which operations the user is authorized to perform.

The Tenant Management Console can also be used to configure the IP addresses, which are permitted to access each namespace.

Default Namespace Data Access

The network services that provide access to the *default* namespace provide very strong authorization controls to compensate for the relative absence of authentication mechanisms.

A system administrator can use the Tenant Management Console to enable or disable any of the network services. When a service is disabled, its port is closed at the HCP firewall and the daemon that would normally respond on that port does not run.

The Tenant Management Console can also be used to limit the IP addresses, which are permitted to access each service. For all services except NFS, these limits can also be configured to explicitly deny service to specific IP addresses. Each service carries its own set of IP address allow and deny settings.

Console Access

The *install* account is used to perform limited software installation and upgrade tasks at the console of the HCP nodes. This is a captive account that provides a menu system for performing the supported operations. Access to the login password of the *install* account should be limited to authorized persons.

No other accounts are authorized for access at the console. Specifically, *root* or *super-user* access is not available under any circumstances.

Service Access

The System Management Console of the HCP system can be used to authorize service access over *ssh*. Such authorization opens the HCP firewall at the *ssh* port (22) and can be restricted to specific IP addresses.

The *service* login account is not a super-user account. However, it does allow the use of *sudo* to escalate privilege for operations, such as starting or stopping a node and mounting and unmounting storage volumes.

Encryption

There are a number of places where encryption technology is used in the Hitachi Content Platform.

Data at Rest Encryption

HCP provides an install-time option to use encrypted block storage for HCP. There are a number of block ciphers available for this purpose. When enabled, the block devices used by HCP are encrypted at all times. Data is decrypted on the fly during reads.

The encryption key used for the data at rest encryption feature is cryptographically distributed among the nodes of the archive using a Shamir secret-sharing algorithm, which requires N or M nodes to be available before any of the storage volumes can be accessed. This severely limits the benefit that can be gained from stealing a RAIN node or a small number of SAN RAID groups.

Data Transmission Encryption

SSL Encryption of HTTP/WebDAV Traffic

All interactions with the System Management Console are SSL-encrypted. The System Management Console is only accessible by HTTPS.

All interactions with the Tenant Management Consoles are SSL-encrypted. The Tenant Management Consoles are only accessible by HTTPS.

When a new namespace is created it can only be accessed by HTTPS. An administrator can use the Tenant Management Console to enable nonencrypted access via HTTP or independently disable HTTPS.

HCP provides mechanisms for generating self-signed certificates, uploading signed certificates and for generating certificate signing requests.

SSL Encryption of Replication Traffic

HCP supports the replication of one or more namespaces to a remote HCP. The tenant administrator has the option of enabling SSL encryption for the replication data stream.

OpenPGP Signing or Encryption of NDMP Traffic

The Tenant Management Console for the *default* tenant can be used to configure OpenPGP encryption for data being exported from HCP using the NDMP service. NDMP dumps can be configured to be compressed, signed, encrypted or any combination thereof.

OpenPGP Encryption of Diagnostic Data Dumps

HCP provides the ability for a user with the *administrator* role to use the System Management Console to extract low-level diagnostic information from a system. This may include detailed logging and configuration information that exposes information about objects in the repository. To safeguard this exposed data, diagnostic dumps are encrypted with the public side of an OpenPGP key pair that ships with the system. The HCP Engineering Team can use the private side of this key pair to decrypt the logs once they have been secured at the Hitachi Data Systems development facility.

Auditing and Monitoring

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.

Hitachi Content Platform event logging is quite extensive. Events of security interest to an HCP system administrator are:

- Changes to the configuration of any service
- OpenPGP key uploads or deletes
- Replication SSL 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
- SSL certificate upload or generation or certificate signing request (CSR) generation
- NDMP signing or encryption key uploads or deletes
- Network Service started/stopped/enabled/disabled
- Tenant creation or deletion

There are a number of security events of interest to a tenant administrator as well:

- 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

Hitachi Content Platform Security Best Practices

This section outlines techniques that can be used to maximize the benefits of the security features provided by the Hitachi Content Platform.

Physical Security

The HCP software cannot protect against a dedicated malefactor with physical access to the servers, switches and storage systems that make up the HCP physical plant. Access to the HCP servers, switches, cabling and storage systems should be restricted to a small number of trusted and qualified persons.

Consider using the data at rest encryption to safeguard sensitive data from accidental disclosure should equipment be removed from your facility.

System Management

The System Management Console provides access to very powerful capabilities, which have a direct effect on the security of the system and the resulting integrity and availability of your data. Limit the use of the security role and plan the use of the administrative roles to limit the possibility of accidental or malicious misconfiguration of the system.

There is a system-wide permissions mask. Use it to set limits on the kinds of operations the system will accept.

Review the system event log frequently for suspicious security-related events.

Tenant Management

The multitenant mechanism is a powerful tool for segregating data from differing business and

management domains. Administrators should plan use of tenants and namespaces to augment business rules for access to data. For example, engineering data and personnel data should be stored in separate namespaces, if not in separate tenants.

As with system management, limit the use of the security role among tenant accounts and take care in granting roles to administrative users.

There are tenant-wide and namespace-specific permissions masks. Use these to disable unwanted types of access at tenant and namespace levels.

Create data access accounts for each application or user that you intend to access each tenant. Use the per-user permissions mask to limit the capabilities of each user.

Review the tenant event log frequently and track down the source of any suspicious activity.

Service Management

Every tenant provides mechanisms for enhancing data access security. Consider the following guidelines:

- Secure HTTP access in all namespaces by enabling SSL and disabling plain HTTP access.
- Secure all network access by limiting the IP addresses that are authorized to connect to any network service.
- If the default namespace is in use, disable any network services that are not being used, including service ssh access and Internet Control Messaging Protocol (ICMP) ping response.

Conclusion

Hitachi Content Platform provides strong support for a full set of industry standard security measures. When its advanced content management features are exploited, HCP is a superior solution for managing and safeguarding the information that powers your business.

 **Hitachi Data Systems Corporation**

Corporate Headquarters

750 Central Expressway
Santa Clara, California 95050-2627 USA
www.hds.com

Regional Contact Information

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

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

All other trademarks, service marks and company names in this document or website are properties of their respective owners.

Notice: This document is for informational purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems Corporation.

© Hitachi Data Systems Corporation 2010. All Rights Reserved. WP-391-A DG December 2010