Hewlett Packard Enterprise

Technical white paper

Check if the document is available in the language of your choice.

DATA SERVICES CLOUD CONSOLE SECURITY GUIDE

CONTENTS

EXECUTIVE SUMMARY

Hewlett Packard Enterprise believes that the future of IT infrastructure lies with data services in the cloud. **Data Services Cloud Console** is a key element of the effort to build the data center infrastructure of the future. This paper describes how Data Services Cloud Console enforces all aspects of data security—from the data center to the cloud.

Data Services Cloud Console was built with a vision of security in mind, focusing on three key requirements:

- **Trusted:** Data Services Cloud Console and HPE Storage array
  - Both Data Services Cloud Console and HPE Storage arrays have third-party signed certificates that verify authenticity.
- **Encrypted:** in and through the cloud
  - All data—both within Data Services Cloud Console and transmitted—is protected by firewalls, authentication, encryption, load-balancers, auditing, vaults, security officers, secure tunnels, and other recommended security practices.
- **Multi-tenant:** separation for safety
  - The data of each Data Services Cloud Console customer is isolated from that of other tenant companies, providing privacy and data access protection.

No data from HPE Storage arrays (such as application data or snapshots) is ever sent to Data Services Cloud Console. Data Services Cloud Console cannot initiate a connection to the HPE Storage array. The connection is always initiated by the HPE Storage array.

Hewlett Packard Enterprise also offers industry-leading service capabilities that provide enterprise-level security support for establishing secure data and controlled access.

Target audience

The target audience for this document includes corporate security personnel, risk planners, and array administrative personnel who will be working with Data Services Cloud Console.

This paper helps Management understand the quality drivers that create a secure product development environment. It provides security personnel and risk planners information about the standards used to develop the product. It offers administrative personnel an overview of the details of how Data Services Cloud Console is accessed and how it shares access and configuration information.

Readers should be familiar with computer concepts associated with management, networking, security, and data storage arrays, as well as with the needs and requirements of their organization and its infrastructure.

Document purpose

This paper describes how Hewlett Packard Enterprise developed Data Services Cloud Console and its associated products to meet your security needs. It is not intended to replace product manuals, but rather to offer an overview of how Data Services Cloud Console provides a secure platform on which customer arrays, and the data they contain, can be securely accessed.

The flow of this paper takes you through an architectural view, outlining how Data Services Cloud Console secures your information across all aspects of the journey—from the cloud to on-premises storage.

After reading it, you will understand how the security capabilities of Data Services Cloud Console are enabled and implemented. If you have additional questions or observations related to this paper, contact your Hewlett Packard Enterprise representative.

OVERVIEW

Data Services Cloud Console is a secure cloud application that provides a control plane for simplifying data infrastructure and delivering unique data services across edge-to-cloud environments. It is deployed on proven technology derived from the HPE Aruba Central cloud management solution. Figure 1 shows an overview of the cloud services available.

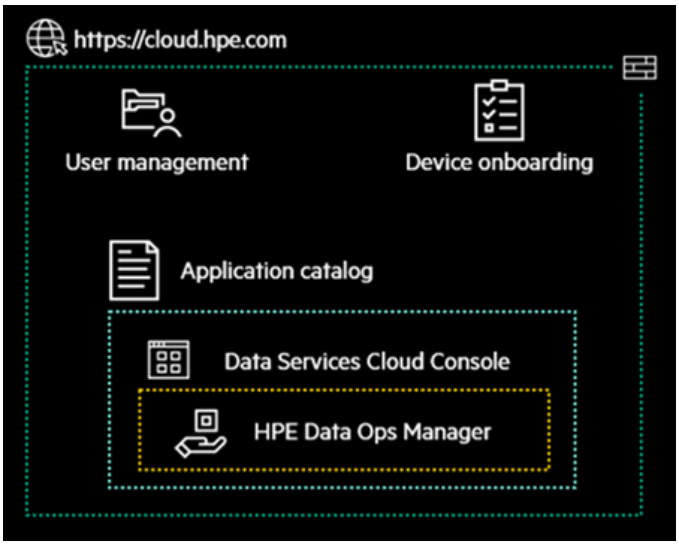

FIGURE 1. Data Services Cloud Console overview

The Data Services Cloud Console application contains software-as-a-service (SaaS) offerings such as **HPE Data Ops Manager**, one of the services that enables global storage management.

Figure 2 shows the capabilities and options that **cloud.hpe.com** offers customers to enable them to customize their authentication preferences to securely manage their HPE storage through the Data Services Cloud Console application services. As shown in the figure, the connections between Data Services Cloud Console and the HPE Storage array are always initiated by the HPE Storage array.

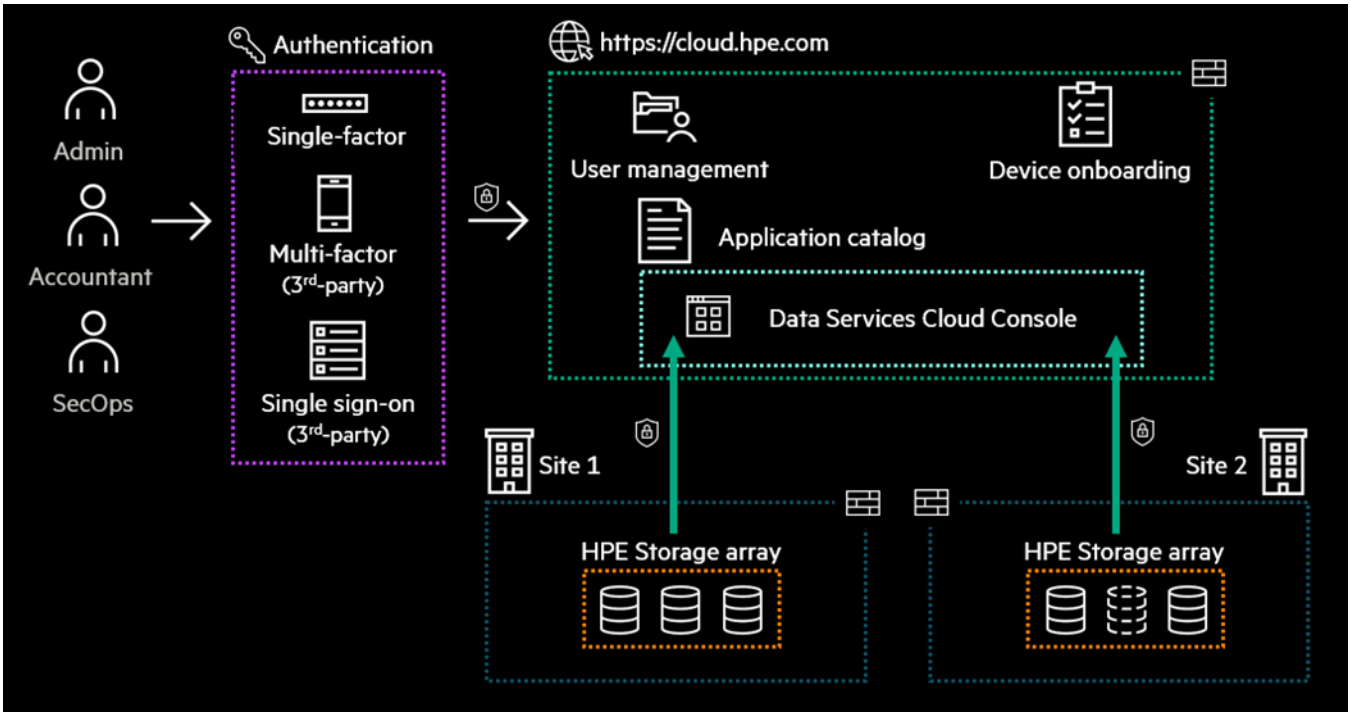

FIGURE 2. cloud.hpe.com security overview

NOTE
Data Services Cloud Console inherits the cloud security framework enforced by **cloud.hpe.com**.

DATA SERVICES CLOUD CONSOLE SECURITY

This paper discusses the security benefits that Hewlett Packard Enterprise provides to its customers through Data Services Cloud Console.

User account

To take advantage of **cloud.hpe.com**, you must have a user account. The user account requires you to enter your name, your email address, and a user name.

After a new user account is verified, you must create or join the account to an organizational unit, which requires entering an organization name and address.

NOTE

All user account and organizational information created in **cloud.hpe.com** is stored in the United States.

Hewlett Packard Enterprise respects and takes into account the major privacy principles and frameworks around the world, including, but not limited to, the OECD Guidelines on the Protection of Privacy and Transborder Flows, the EU General Data Protection Regulation 2016/679 (GDPR), and the APEC Privacy Framework. The HPE privacy practices described in this Privacy Statement also comply with the APEC Cross Border Privacy Rules (CBPR) System. For more information, see the Hewlett Packard Enterprise Privacy Statement.

The creator of an organizational unit is assigned administrator privileges for that organization with the option of inviting additional users and configuring access permissions. Additional users can request access to the organizational unit; however, no access is granted until the administrator approves the request with appropriate permissions.

NOTE

If single sign-on (SSO) authentication is configured, invited users will not require a **cloud.hpe.com** user account to be created.

A single user account can create or join multiple organizational units. Because **cloud.hpe.com** is a multi-tenant environment, it allows users to access only the information that belongs to their assigned organizational units.

To take advantage of all that Data Services Cloud Console has to offer, a valid serial number and an entitlement ID are required. (The serial number and entitlement ID are received during the HPE Alletra purchase.)

If a user no longer requires access to **cloud.hpe.com** and Data Services Cloud Console, the administrator can disable the user's account. For traceability and compliance, audit logs referencing the user remain unchanged to accurately reflect actions performed by that user. Hewlett Packard Enterprise recommends that organizations include the removal of **cloud.hpe.com** accounts in their employee offboarding process.

Authentication

Hewlett Packard Enterprise will provide three types of authentication for logging into **cloud.hpe.com**:

- Single-factor authentication
- Multi-factor authentication
- Single sign-on (SSO)

Single-factor authentication

Single-factor authentication requires a user name and password to verify a user's identity.

Passwords must meet the following specifications:

- Must be between 8 and 255 characters, with a minimum of five unique characters
- Cannot have more than two repeated characters
- Must contain at least one special character, one numeric character, one uppercase letter, and a lowercase letter
- Cannot contain user account data and are checked against a list of commonly used passwords

All validated passwords adhere to a strict policy:

- New passwords cannot match the past six passwords used within the past 365 days.
- Passwords expire automatically after 182 days.
- Accounts with multiple login failures are automatically locked out for a period of time.

Multi-factor authentication

Multi-factor authentication implements multiple levels of authentication for a user to gain access to **cloud.hpe.com**. This capability will be made available to customers shortly after the initial launch.

Hewlett Packard Enterprise will support software-based authenticators (such as those from Google™ and Microsoft) that, when combined with a traditional user login, provide an extra layer of security, as shown in Figure 3.

FIGURE 3. Software-based authenticator login process

Single sign-on authentication

SSO authentication enables organizations to simplify the user experience of logging into external portals by allowing users to enter their company login credentials to authenticate their identity. This capability will be made available to customers shortly after the initial launch.

As Figure 4 shows, users will be able to log into **cloud.hpe.com** with their company user credentials. After their login, however, **cloud.hpe.com** will verify those credentials by sending a SAML request (digitally signed XML) to the user's trusted company identity provider (IdP), which in turn will verify the credentials and send back a SAML response confirming that they are valid.

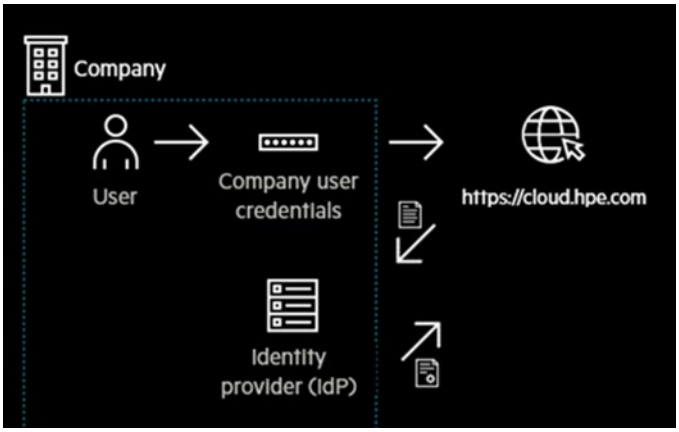

FIGURE 4. SSO login process

NOTE

With SSO, a **cloud.hpe.com** account is not required if a user is invited by the organizational unit administrator, allowing them instant access into **cloud.hpe.com** with their company user credentials. In addition, if a user account is disabled, access to **cloud.hpe.com** is revoked.

User permissions

Cloud.hpe.com user permissions are enforced by using **role-based access control (RBAC)** to ensure that the correct level of access is given to each user. The administrator of an organizational unit has the option to assign predefined roles provided by **cloud.hpe.com** or to create custom roles for users. Table 1 lists examples of predefined roles offered within **cloud.hpe.com**.

NOTE
The creator of the organizational unit within **cloud.hpe.com** is automatically assigned administrator permissions.

TABLE 1. cloud.hpe.com role examples

Role	Assigned permissions
System admin	All permissions available to set up and configure **cloud.hpe.com** settings and application-level actions (array functions)
Power user	Application-level actions except for system edit and update
Operator	Application-level actions, create and edit functions, but no delete
Guest	View-only access (no ability to execute any actions)

Role assignment

Cloud.hpe.com role assignments offer a diverse selection of permission options available to the administrator. In example shown in Figure 5, the administrator can associate multiple assignments to a single user, with each assignment consisting of a range of **roles**, such as Systems Admin (a predefined collection of permissions), and **scopes**, for example, EU Region (only European resources accessible).

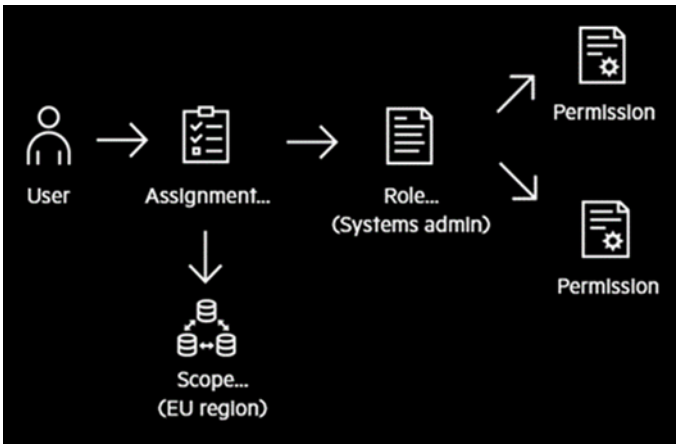

FIGURE 5. Role assignment example

Table 2 lists the permissions terminology used in **cloud.hpe.com**.

TABLE 2. cloud.hpe.com permissions terminology

Type	Assigned permissions
User	A **cloud.hpe.com** user account
Assignment	A list of roles and scopes
Role	A list of permissions
Permission	Examples are create, edit, and delete functionality
Scope	A list of resources that are affected by the roles assigned (for example, only resources in the EU region can be edited)

NOTE
Only HPE Authorized Engineers with customer consent have access to customer accounts for support troubleshooting. This access can be revoked at any time by the customer.

Data collection

Data collection, together with data residency and sovereignty, is a growing concern in any SaaS solution. Hewlett Packard Enterprise addresses these issues:

- **cloud.hpe.com** retains specific company data to provide high-quality services, and protecting this data is a top priority.
- **cloud.hpe.com** stores user and organizational account information in the United States, adhering to all privacy and security regulations.
- Data Services Cloud Console application data is stored at the region level, adhering to data residency and sovereignty concerns.
- Customer data (data stored on array volumes or LUNs) is never sent to Data Services Cloud Console.
- Data Services Cloud Console data collection is limited strictly to configuration and performance-related data.

NOTE
Data Services Cloud Console application is available in multiple regions, including the United States of America (US), Europe (EU), and Japan (JP).

Table 3 lists the information retained by **cloud.hpe.com**.

TABLE 3. Data collected

Location	Information	Details stored
cloud.hpe.com	User details	Name, email address, and user name
cloud.hpe.com	Organizational details	Name, address, and contact details
Data Services Cloud Console	Device inventory	Product family, model, system WWN, software version, capacity utilization, controller details, volume information, and snapshots

Distributed denial of service

Distributed denial of service (DDoS) is a malicious attempt to disrupt network communication, preventing a website from functioning correctly and denying access.

Data Services Cloud Console inherits **cloud.hpe.com** DDoS protection services, combining an intelligent web application firewall (iWAF) with load balancing, rate limiting, intrusion protection, and a threat-monitoring security service, as shown in Figure 6.

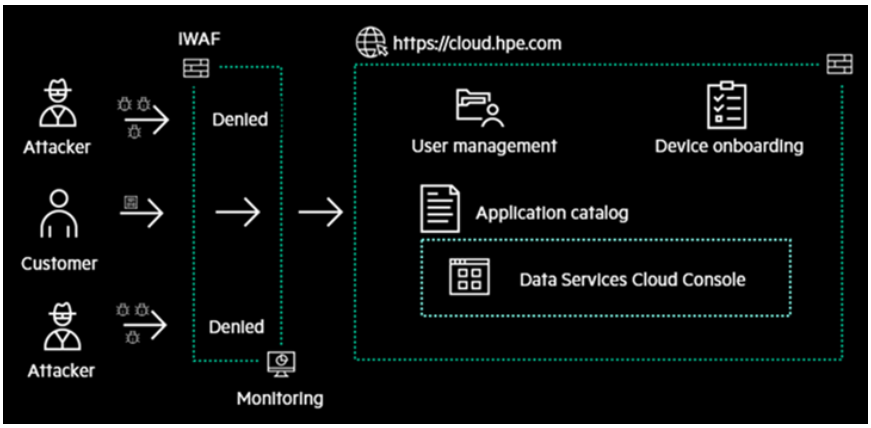

FIGURE 6. DDoS example

Audit logging

Audit logs are an essential security tool for providing records of all events and changes that occur within a system or environment.

Data Services Cloud Console **audit log service** provides a comprehensive audit trail to assist in monitoring potentially sensitive data or systems for possible security breaches, vulnerabilities, or misuse of data. It also provides records that serve as evidence in cybersecurity attacks. In addition, audit logs may be considered business records that prove compliance to regulations and the law.

Data Services Cloud Console audit log access is customer configurable to allow regular auditor checks for compliance purposes.

Table 4 provides a sample of audit log details.

TABLE 4. Data Services Cloud Console audit log example

Content	Description	Example
Who	The user who initiated the action	John Doe
Where	The source of the request	10.10.10.10
When	The timestamp when the request was made	2020-05-05 12:30
What	The action requested	Login attempt
Outcome	The result of the request	Failed

NOTE
Each Data Services Cloud Console application instance deploys a separate audit log.

Secure sites

Customer secure sites typically contain systems that do not and cannot communicate with other devices outside the customer's internal network.

On-premises storage systems are required to have a connection to **cloud.hpe.com** for activation and to Data Services Cloud Console for software and firmware updates. Support is under development, and Data Services Cloud Console deployments locally and into cloud services such as AWS GovCloud (for government agencies) are undergoing development and certification compliance checks.

API support

Hewlett Packard Enterprise plans for Data Services Cloud Console to provide a rich set of public RESTful APIs designed to drive customer agility to swiftly achieve their goals. The RESTful API plans are to include all storage array resources and capabilities of Data Services Cloud Console, leveraging HTTPS security tokens (obtained through user authentication with Data Services Cloud Console) to keep communications secure.

Compliance and certification standards

Hewlett Packard Enterprise is focused on ensuring that HPE systems are secure, compliant, and certified:

- Data Services Cloud Console and **cloud.hpe.com** have been tested and have passed Privacy Compliance and Impact Assessment reviews.
- Data Services Cloud Console has undergone security penetration testing by external vendors.
- Data Services Cloud Console is aligning with multiple compliances and certifications.

User and site public interfaces

Connecting to Data Services Cloud Console either from a user's web browser or from the HPE Storage array requires access to the public interfaces of Data Services Cloud for users to take advantage of the services it provides. It requires two types of public interfaces to be accessible, as shown in Figure 7 and detailed in Table 5. The customer's network proxy or firewall must allow outbound connections to these public interfaces.

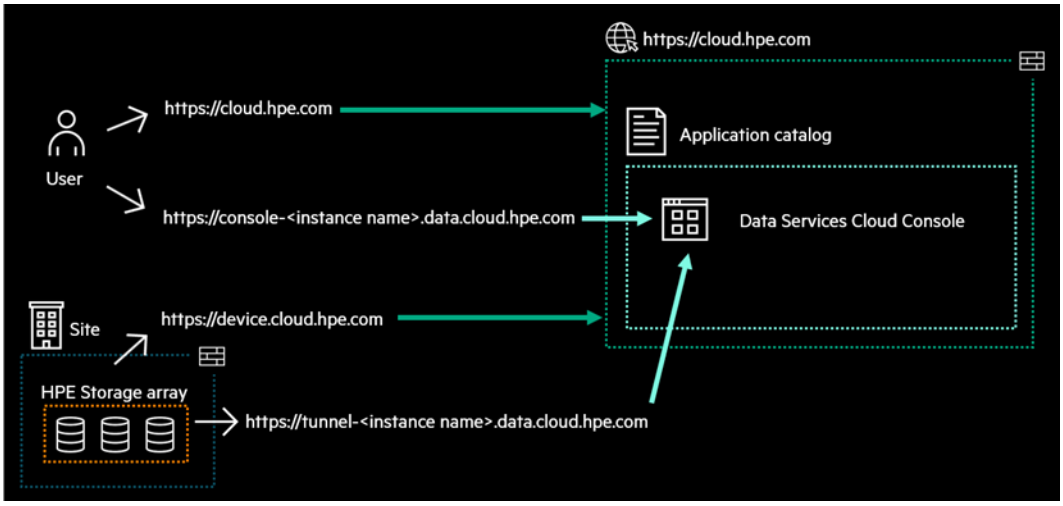

FIGURE 7. Data Services Cloud Console public interfaces

TABLE 5. Data Services Cloud Console public interfaces

Public interface FQDN	Port	Initiator	Description
https://cloud.hpe.com	443	User	Allows communication to cloud.hpe.com
https://console-<instance name>.data.cloud.hpe.com	443	User	Allows communication to Data Services Cloud Console instance (Europe: **eu1**, Japan: **jp1**, America: **us1**) For example, **https://console-eu1.data.cloud.hpe.com**
https://device.cloud.hpe.com	443	HPE Storage array	Required for activation only
https://tunnel-<instance name>.data.cloud.hpe.com	443	HPE Storage array	Allows communication to Data Services Cloud Console instance (Europe: **eu1**, Japan: **jp1**, America: **us1**) For example, **https://tunnel-eu1.data.cloud.hpe.com**

NOTE

HPE Storage arrays might require network proxy information to be configured to access Data Services Cloud Console public interfaces.

Secure communication with the cloud

Data Services Cloud Console is a control plane that facilitates all management communication for HPE Storage arrays. A secure communication link must be established from each HPE Storage array for all communication with Data Services Cloud Console.

IMPORTANT

The request for a secure connection is always initiated by the HPE Storage array and never by Data Services Cloud Console. It is not possible for Data Services Cloud Console to initiate a new connection to the HPE Storage array.

Table 6 lists the terminology used in this section.

TABLE 6. Terminology

Term	Description
On-premises device	HPE Storage array located at the customer site
Northbound	Information sent from on-premises device to Data Services Cloud Console through the tunnel
Southbound	Information sent from Data Services Cloud Console to the on-premises device through the tunnel
mTLS	Mutual Transport Layer Security
Tunnel	Bidirectional secure and encrypted communication pipeline initiated by on-premises device

All northbound and southbound communication requires an active secure tunnel, created by using mTLS, as shown in Figure 8.

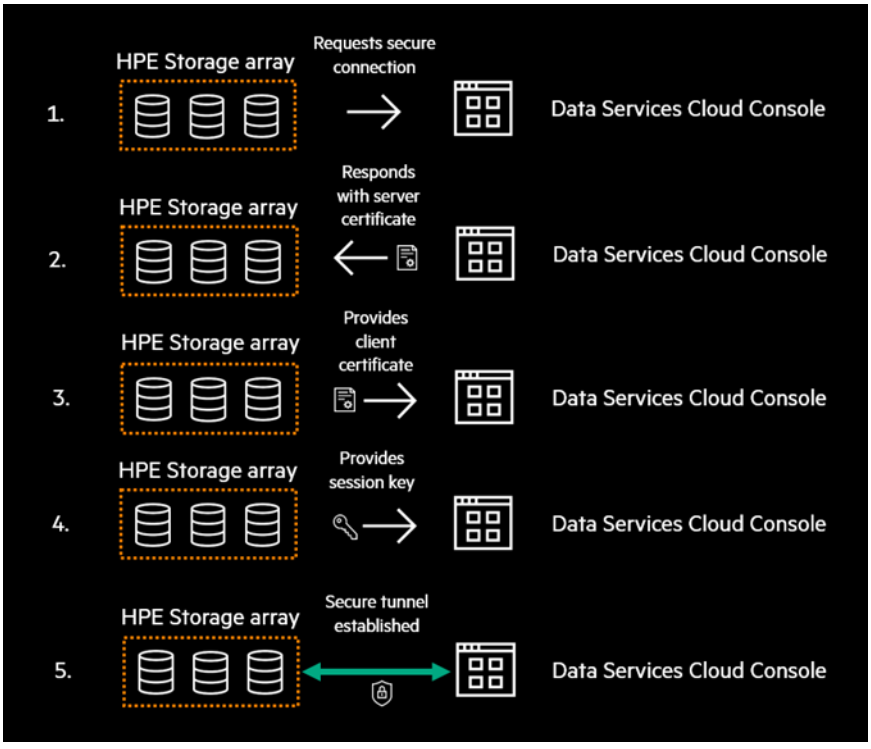

FIGURE 8. Data Services Cloud Console mTLS secure tunnel steps

NOTE

HPE Storage arrays contain a certificate signed by a trusted certificate authority and installed during the manufacturing process.

The request for a secure connection is always initiated by the HPE Storage array and never by Data Services Cloud Console, as shown in Figure 9.

After a secure tunnel is established between the on-premises device and Data Services Cloud Console, it remains active to send northbound management event data and southbound Data Services Cloud Console management requests (RESTful API calls).

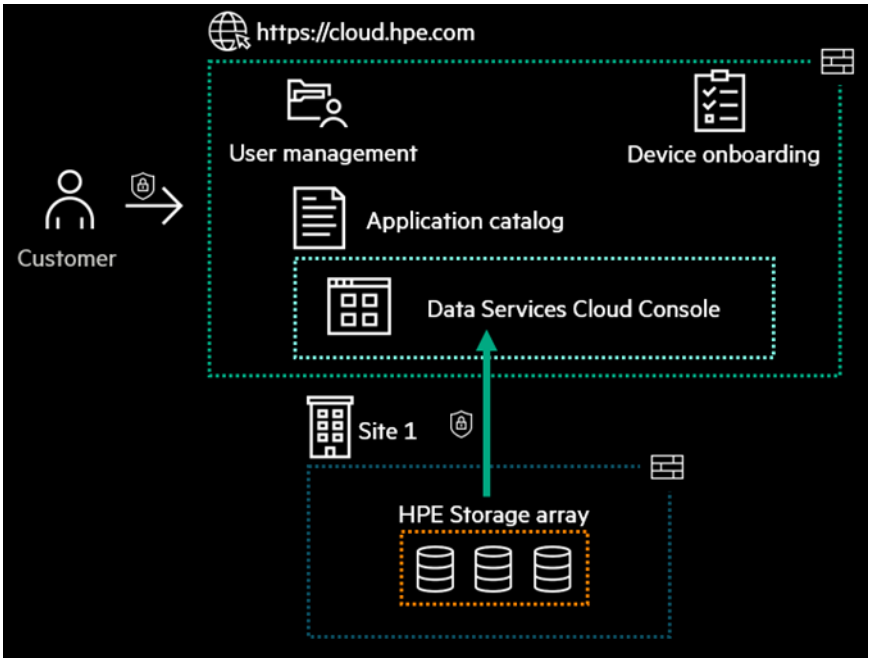

FIGURE 9. Data Services Cloud Console secure communication

Data Services Cloud Console communication performance and high availability are key. One way these goals are achieved is by adopting load balancers to prioritize all incoming traffic to Data Services Cloud Console instances. In the event of a communications disconnect between Data Services Cloud Console and HPE Storage array, the HPE Storage array automatically begins the process of re-establishing a new connection (by generating a new session key) to Data Services Cloud Console. After the connection is re-established, any queued northbound events since the disconnect are then transmitted.

Device onboarding

HPE Storage arrays require onboarding within **cloud.hpe.com** before the Data Services Cloud Console application services can manage the HPE Storage array.

NOTE

For information about how to allow communication access to the activation FQDN, see the User and site public interfaces section of this paper.

The onboarding process requires an HPE Storage array **serial number** and a Data Services Cloud Console **subscription key** to be registered with **cloud.hpe.com**. After **cloud.hpe.com** onboarding is complete, the HPE Storage array can create a secure mTLS tunnel to **cloud.hpe.com** for activation.

Management types

HPE Storage arrays enable customers to take advantage of different management types to suit their environment (through the array management GUI, the CLI, RESTful APIs, plugins, and so forth). Data Services Cloud Console enhances the customer experience and provides a unified approach to storage management. To enforce user security on Data Services Cloud Console, users that are created on the HPE Storage array do not gain access or equivalent permissions within Data Services Cloud Console.

NOTE
Customer data (data stored on HPE Storage array volumes or LUNs) is never sent to Data Services Cloud Console, and it is not possible to open a CLI or shell session on the HPE Storage array from Data Services Cloud Console.

Application credentials

HPE Storage arrays are likely to require credentials to access and interact with other applications. Customers can provide application credentials of this nature to Data Services Cloud Console, where they are stored and protected in a secure credential vault.

Shared security control

Both Hewlett Packard Enterprise and the customer have a part to play in controlling security—either in the cloud (where Hewlett Packard Enterprise prevents unauthorized access to user profile data) or at the customer site (where the customer prevents unauthorized access to IT hardware). Figure 10 illustrates how security is implemented and who retains responsibility for specific security mitigation controls.

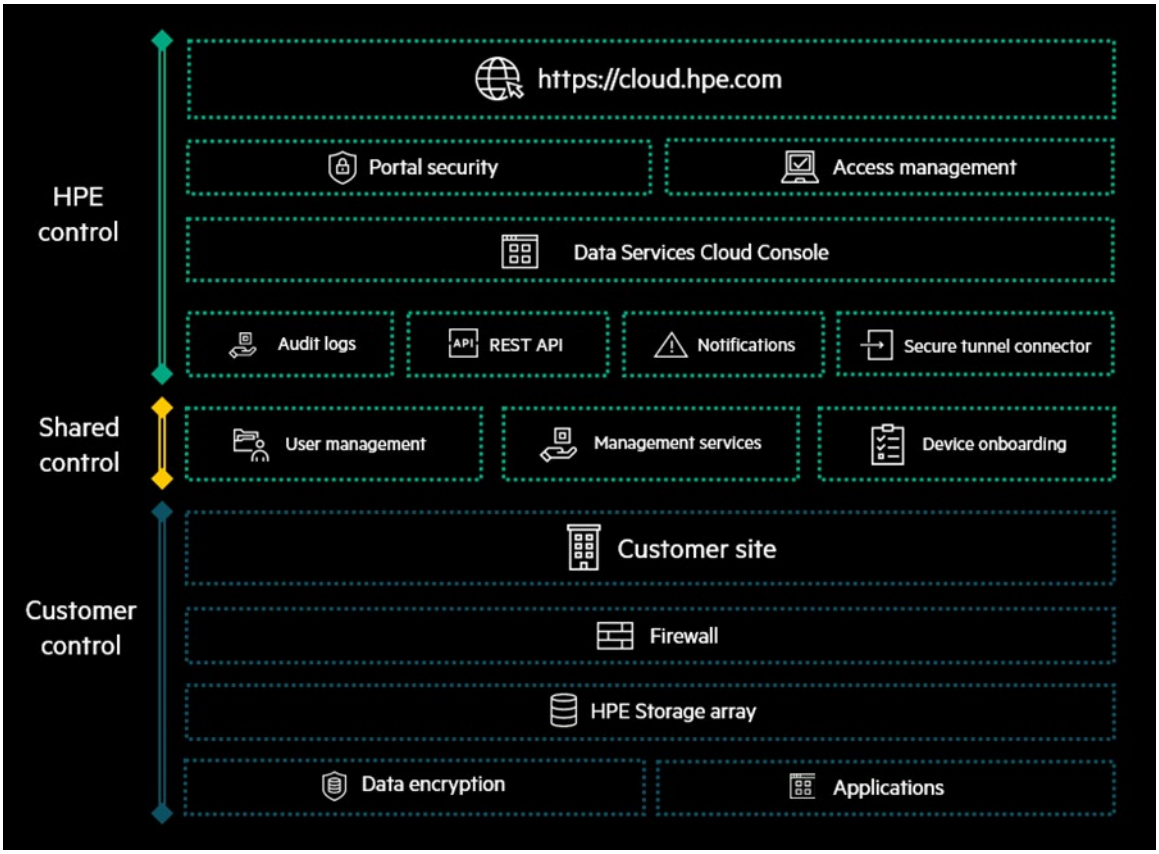

FIGURE 10. Data Services Cloud Console security control

Hewlett Packard Enterprise follows best practices for SaaS hosting, which include cloud security tools (firewalls, distributed load-balancers, and auditing) and other recommended best practices.

Both the customer and Hewlett Packard Enterprise share a portion of control over the securing of user credentials for accessing Data Services Cloud Console. Responsibilities include using strong passwords, allocating appropriate privileges, removing users who have left the company, and restricting device onboarding information.

Customers are responsible for their premises, for access to the company network, for access to the HPE Storage array containing encrypted volumes, for hosting customer applications, and for implementing other recommended best practices.

SUMMARY

Your organization needs to have confidence that your infrastructure components, such as your data storage arrays, can meet and maintain your organization's security policies. Security involves all aspects of the IT infrastructure—from the very smallest component of a machine up through the collection of computing devices in the data center, their connectivity, and the way all of these components are managed by using the cloud.

HPE products are required to be capable of operating in secure environments without allowing information to be compromised by limitations in product capabilities, quality, or operation. Such requirements have driven HPE products to achieve superior product quality and capabilities. Hewlett Packard Enterprise has developed Data Services Cloud Console and its associated products to meet your security needs.

Hewlett Packard Enterprise offers industry-leading service capabilities that encompass the requirements for security. It provides on-premises monitoring coupled with multi-device rollup of information to the HPE InfoSight portal for customer-configurable analysis of an enterprise.

Hewlett Packard Enterprise also understands that organizations cannot have unbridled access to their environment. All machinery is configured by using a least-privilege level of access, and all access is controlled by the customer. Therefore, customers determine which service personnel can have access to their machinery and when that access can occur. With software based on these principles, the security of your information is always under your control.

Resources, contacts, or additional links

For more security information, see the HPE Alletra manuals.

LEARN MORE AT

hpe.com/storage

Make the right purchase decision.
Contact our presales specialists.


Chat


Email


Call


Get updates

a00113337ENW, May 2021, Rev 1

Hewlett Packard Enterprise