HPE Alletra Storage

Technical white paper

HPE Alletra Storage MP B10000 security guide

HPE GreenLake

Contents

Executive summary

Security concerns plague the corporate environment daily. New threats, old threats, hacks, and outright nefarious actions threaten corporate data at alarming rates. Robust security controls are required to protect an organization's data from negative outcomes such as unauthorized access, data breaches and physical theft, and accidental or intentional data loss. There is a myriad of threats to an organization's data, from external threat actors executing ransomware attacks or denial of service attacks to internal threats, both intentional and accidental. Ransomware is particularly troubling and is quite rightly at the forefront of the minds of many security and IT professionals. Ransomware refers to malicious software (malware) that is deployed within an enterprise's infrastructure without the company's knowledge, encrypting data until the attacker chooses an opportune moment to demand a ransom payment. These attacks have evolved in sophistication and the level of damage they cause, employing methods that make them harder to detect and more difficult to recover from. By encrypting or deleting backup data, attackers attempt to render recovery efforts useless, increasing the chance of the affected party paying the ransom.

IT security professionals must consider threats from every possible angle and ensure that their systems, networks, and data are properly protected through comprehensive security policies that cover everything from access and authorization to backup and disaster recovery.

The purpose of this technical paper is to acquaint the reader with the wide range security features of HPE Alletra Storage MP B10000 arrays to help customers protect their data, prevent unauthorized access to the storage array, and comply with U.S. federal security mandates. This paper explains the many security features used in HPE Alletra Storage MP B10000. The following topics are covered:

- HPE security architectural standards
- Storage environment protection
- Detection of vulnerabilities in storage environments
- Ransomware prevention and recovery

Target audience

This technical paper is designed for corporate security staff, risk strategists, and storage administrators who work with HPE Alletra Storage MP B10000 arrays. The security features described in this document relate to the HPE Alletra Storage MP B10000 v10.5.0 release, previous releases may not support all features described and it is strongly recommended to update to the latest release.

Secure development and supply chain

This section discusses the engineering and manufacturing processes used by Hewlett Packard Enterprise, such as secure development, secure supply chain processes, U.S. federal certifications and validations, the HPE anti-counterfeiting program, and HPE packing and labeling authentication.

HPE works to ensure that its factories have strict access control measures and physical security protocols in place to safeguard physical and informational resources from unauthorized access. Code signing, malware scanning, and vulnerability analysis are mandated in the HPE secure software development lifecycle. HPE security procedures include the following standards:

- Software loaded onto HPE products in HPE manufacturing facilities is scanned for malware.
- HPE code delivered to customers is digitally signed.
- No HPE product may have a known back door or an unauthorized communication channel mechanism that would allow unauthorized access to the device.
- As part of the release to production process, all firmware, including system BIOS, is digitally signed at the development stage.
- All HPE Alletra Storage MP B10000 products are compliant with the Trade Agreements Act (TAA), meaning they are manufactured or substantially transformed in the USA or a TAA-designated country.

Cybersecurity Supply Chain Risk Management

The Cybersecurity Supply Chain Risk Management standard establishes a set of requirements of a risk management system for the HPE supply chain focused on cyber related threats. The main objectives are:

- To establish a risk management system with clear roles and responsibilities for cyber risk management activities in the supply chain across all Business Units.
- To have standard methodologies to address the ever-changing cyber threat landscape and manage cyber risks in the supply chain

All new product introductions follow a four-step risk management methodology to manage cyber risks in the supply chain:

1. Frame
2. Assess—perform a threat and vulnerability analysis, determine the likelihood of a vulnerability exploit, perform impact analysis and assessment
3. Respond—determine the action, and select and implement appropriate controls
4. Monitor—evaluate the effectiveness of controls implemented in the Respond step

HPE anti-counterfeiting program

HPE anti-counterfeit (ACF) investigation and enforcement (I&E) confronts all touchpoints of the counterfeiting industry—everything from the smallest suppliers to the largest counterfeit packaging and component fabricators, distributors, and manufacturers. HPE ACF I&E collaborates with law enforcement agencies and customs officers all over the world to combat the trafficking of counterfeit items. The HPE counterfeit intelligence team draws on the expertise of police officers and professionals when investigating the traffic of illicit products.

HPE ACF I&E sends out highly competent, seasoned investigators to stop counterfeiting activities throughout the world. Law enforcement agencies conduct on-the-ground seizures using HPE information, and local governments pursue appropriate punishment through the criminal justice system.

HPE pursues further sanctions through civil lawsuits in addition to criminal seizures. HPE is a member of Business Action to Stop Counterfeiting and Piracy (BASCAP), a worldwide leadership organization convened by the International Chamber of Commerce to safeguard intellectual property and prevent counterfeiting.

HPE packaging and labeling authentication

HPE employs security labels with high-tech elements that lead to confident product authentication. To maintain package integrity during shipping, product packaging is commonly sealed with a tamper-evident security label. Tamper-evident packing tape is applied to the outside of the shipping box.

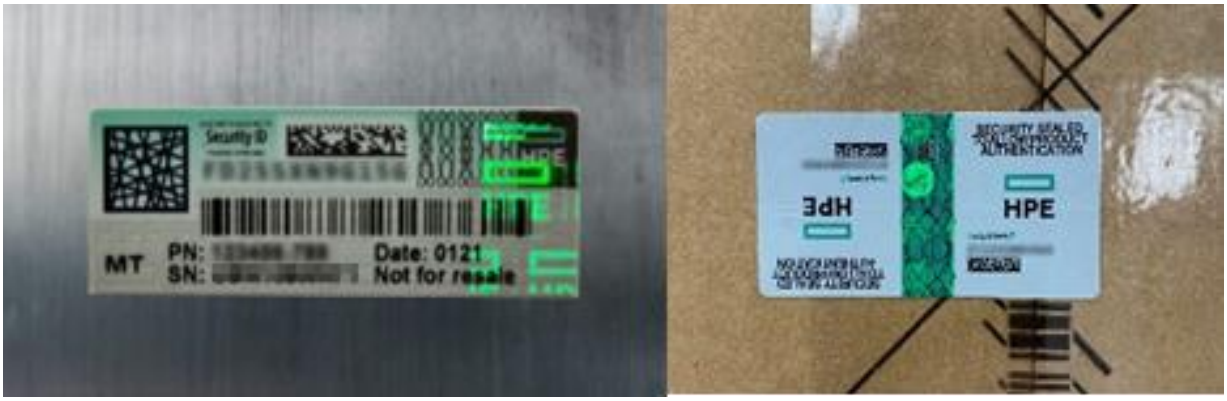

Figure 1. Labeling authentication (left) and packaging (right)

Penetration testing and vulnerability scanning

HPE partners work with third-party companies to perform extensive penetration testing on every major release of HPE Alletra Storage ArcusOS during product development. In addition to the third-party pen-testing, HPE performs in-house vulnerability assessment and remediation against common vulnerabilities and exposures (CVE) to help ensure the software is free from known vulnerabilities and to protect both the partner's customers and HPE customers.

Across the company, HPE maintains a product security response team (PSRT), part of the Product Security Office, which is responsible for receiving, tracking, managing, and disclosing vulnerabilities in HPE products. When vulnerabilities are reported, the HPE PSRT works actively with industry, non-profit, government organizations, and the security community to investigate them.

Additional security measures

The following mechanisms are among those used to prevent and remediate threats and avoid negative impacts to HPE or its customers:

- There is a value comparison of secure hash algorithms (SHA), which generate an alphanumeric number, recognized as the code's "fingerprint."

Any modification to the code, no matter how small, such as adding or removing a space, alters the fingerprint value. This procedure helps ensure that what the lab delivers is exactly what goes into production. A SHA-256 fingerprint is automatically validated by the HPE software code repository (SMTA2), then by supply chain product engineering throughout the quality verification check process (post-lab release), and ultimately during the First Article Inspection (FAI) sample review process prior to manufacturing release.

- HPE performs malware scanning using an approved, automated anti-malware tool before releasing product delivery to customers.
- The HPE software code repository, through which HPE software flows to manufacturing, checks software for viruses and malware on a regular basis.
- Restrictions are in place against back doors and illegal communication channels to prevent illicit authentication of digital signatures or use of native signature validation capabilities.
- A detailed system inventory check of software is performed for clients who have software installed in a facility owned or contracted by HPE.
- Apps developed by HPE, and third-party apps, are sent to HPE factories over secure channels and housed in a secure environment where they undergo virus scanning regularly.

U.S. federal certifications and validations

HPE has an ongoing program that prioritizes U.S. federal compliances and certifications.

IPv6

HPE Alletra Storage MP B10000 arrays are listed in the USGv6 registry of approved products, meaning that they are independently tested and certified for use on IPv6-only networks to comply with the U.S. Government Office of Management and Budget Memorandum M-21-07, and subsequent Department of Defense requirements. In addition, HPE Alletra Storage MP B10000 arrays also received the IPv6 Ready Phase 2 (Gold) Core Logo for host accreditation from the IPv6 Forum, an international consortium with a key focus of providing technical guidance for the deployment of IPv6.

Transport Layer Security (TLS)

HPE Alletra Storage MP B10000 arrays support TLS 1.3, which offers improved security for both high performance and improved reliability. The benefits of TLS 1.3 over TLS 1.2 and earlier standards include a faster, more efficient, and more secure handshake, with a simplified key exchange. Removal of outdated and vulnerable hashing algorithms and cryptographic ciphers enables a more refined list of supported cipher suites, supplying only 5 rather than the 37 supported by TLS 1.2. TLS 1.3 meets Payment Card Industry Data Security Standards (PCI-DSS) compliance by ensuring that data provided during a credit card transaction between a web server and web browser remains secure. TLS 1.3 support is also required by NIST (National Institute of Standards and Technology) Special Publication (SP) 800-52 Revision 2 for U.S. public sector organizations.

Federal Information Processing Standards (FIPS)

FIPS are standards and guidelines developed by NIST for U.S. federal computer systems. The FIPS 140 series are security standards used by the U.S. government that specify requirements for cryptographic hardware devices. These certifications and compliances help ensure that the process of specifying, implementing, and evaluating a computer security product is carried out in a rigorous, consistent, and repeatable way, and at a level that corresponds to its intended use environment. Through enabling data-at-rest encryption with FIPS-certified drives and a FIPS-compliant external key manager, and by specifying the cryptographic ciphers in use on the system by enabling FIPS mode, HPE Alletra Storage MP B10000 arrays can meet the requirements set out in FIPS 140-2.

Software Bills of Materials

U.S. Executive Order #14028 requires a Software Bills of Materials (SBOMs) from all U.S. federal government suppliers. U.S. Federal agencies are required to use only software provided by manufacturers who can attest to complying with government-specified secure software development practices and must collect attestation letters for that software. To comply with these requirements, HPE requires that SBOMs be cryptographically signed and tied to a hash of the software build the SBOM represents, providing solid provenance.

HPE Alletra Storage MP B10000 security features

This section discusses the ability of HPE Alletra Storage MP B10000 arrays to protect against malicious attacks by using a variety of enhanced security features.

Strong password protection

HPE Alletra Storage MP B10000 arrays employ a time-based, one-time password or a ciphertext-based encrypted password for all privileged accounts used by HPE Support.

Time-based passwords

Time-based passwords are unique to each service user account for HPE Alletra Storage MP B10000 arrays. Passwords change every hour and can be generated only in an HPE Support Center by authorized HPE employees and contractors. Time-based passwords are designed to be particularly difficult to crack, especially during a replay attack. A malicious agent who obtains a one-time password cannot reuse it later because it expires after a specified period and is not valid for future logins.

Ciphertext-based passwords

Ciphertext-based passwords are random passwords that are generated and encrypted by the array and must be decrypted by HPE Support. These passwords must be exported by the customer and provided to HPE personnel working with the customer. The ciphertext is pasted into an HPE Support tool that can unwrap and decrypt the password. Ciphertext-based passwords are secure because they display a form of the original plain text that is unreadable by humans or computers without the proper cipher to decrypt it. Recovery is possible only by exporting the ciphertext to HPE Support.

Encrypted passwords reduce the probability of malicious agents obtaining any credentials. Encryption-based passwords are scrambled, so if malicious agents were to gain access to the array, they would find only a random string of letters and numbers.

On HPE Alletra Storage MP B10000 arrays, encryption-based passwords are created at random for each service user account. The administrator can change these passwords at any time, but neither the customer nor HPE can read them. An authorized HPE Support Center user can decode the password and provide it to on-site HPE Service professionals or contractors. When the support activity is finished, the administrator can update the password so that the original password is no longer valid.

Virtual Lock

Virtual Lock for HPE Alletra Storage MP B10000 is a mechanism that prevents volumes or snapshots from being deleted, intentionally or unintentionally, before a defined retention period elapses. The administrator can specify the retention period for each volume or copy of a volume, which cannot be reduced or removed once set, and which is enforced by a compliance clock that prevents overrides by changing the system time or NTP servers. Locked volumes or snapshots cannot be deleted, not even by the administrator or HPE Tech Support. Combining Virtual Lock with read-only snapshots helps achieve full immutability, providing unmodified copies of data for restoration if a cybercrime, such as a ransomware attack, were to occur.

Virtual Domains

The HPE Alletra Storage MP B10000 Virtual Domains software is an extension of the block storage's virtualization technologies that delivers secure segregation of virtual private arrays (VPAs) for different user groups, departments, and applications. It also preserves the benefits that massive parallelism delivers while supporting the HPE Alletra Storage MP B10000 multitenancy paradigm.

By providing secure administrative segregation of users and hosts within a consolidated, massively parallel HPE Alletra Storage MP B10000 system, **Virtual Domains** grant administrators the ability to provide logically isolated storage to eliminate unauthorized or accidental access.

Depending on the access level granted, users assigned to Domain A can create, export, and copy volumes in Domain A, but cannot see or access application sets, hosts, or volumes, in other domains. HPE Alletra Storage MP B10000 Virtual Domains is ideal for enterprises or service providers who want to leverage the benefits of consolidation and deploy a purpose-built infrastructure for their private or public cloud.

Self-encrypting drives

HPE Alletra Storage MP B10000 arrays use self-encrypting drives (SEDs) equipped with an ASIC in the chipset that automatically sets encryption and decryption of all data being written to and read from the drive, with negligible impact to performance. Two types of SEDs are available, FIPS-certified SEDs and non-FIPS-certified SEDs. FIPS-certified SEDs support full-disk AES-256-XTS encryption, based on FIPS 140-2 validated SED security Level 2 standards, and comply with NIST and Canadian Communication Security Establishment (CSE) specifications. Non-FIPS-certified SEDs offer the same level of hardware AES-256-XTS encryption, but without the NIST certification. Both FIPS-certified and non-FIPS certified SEDs are supported simultaneously in an HPE Alletra Storage MP B10000 array in an encrypted or non-encrypted mode, where FIPS compliance is not required. SEDs strengthen the physical security of an array by making unauthorized physical access more difficult and easier to detect. To protect the physical encasings, FIPS-certified SEDs leverage a combination of tamper-evident coatings, seals, and pick-resistant locks.

Cryptographic erasure

Traditional non-SEDs are sanitized by overwriting the existing data with ones and zeros one or more times to destroy the data. SEDs use a process known as cryptographic erasure, or cryptoerase, to perform the same function within a matter of milliseconds. The cryptoerase process destroys the media encryption key (MEK) and generates a new one. Although the data still resides on the disk in an encrypted form, destroying the MEK renders it unrecoverable because the key required to decrypt the data no longer exists.

A cryptoerase occurs on an SED when a new drive is admitted to the array by using the **admitpd** command, or when a drive is dismissed from the array prior to removal by using the **dismisspd** command.

Data-at-rest encryption

Self-encrypting drives encrypt the data as it is written by using its MEK, which is maintained securely by the drive and cannot be extracted or read. The data is accessed by the array using an authentication key (AK). SEDs encrypt data as it is written to the drive, even if data-at-rest (DAR) encryption is not enabled on the array.

Enabling DAR encryption on the array changes the authentication key on each drive and enables drive lock, which causes the drive to lock if power is removed, for example, if the drive is physically removed from the array. After power is restored, the drive can be accessed only after the matching AK has been supplied. Enabling DAR encryption has negligible impact on drive performance because SEDs always encrypt all data written through the onboard encryption module. DAR encryption is nondestructive and can be applied to arrays that already contain data because it changes the AK used to access the data. After DAR encryption has been enabled, it cannot be disabled.

Note
Data-at-rest encryption refers to encryption of data stored on self-encrypting drives as opposed to data in transit or data in use.

Data-at-rest encryption: key management

The authentication key (AK) is integral to enabling array-level DAR encryption. If this key is lost, all data on the drives will be lost. The AK is maintained in either a local key manager (LKM) or a third-party external key manager (EKM). If the LKM is in use, all key management is handled locally on the HPE Alletra Storage MP B10000 array through an internal operating system process. If an EKM is used, the AK is created and stored in the EKM, and it is retrieved when needed to unlock drives in the array. With LKM, the encryption key is stored in a locally maintained keystore in the array.

When encryption is enabled on an HPE Alletra Storage MP B10000 array, it creates a backup of the keystore. Backup actions for encryption keys are accessible in the HPE Alletra Storage MP B10000 UI or in Data Services Cloud Console. HPE Alletra Storage MP B10000 arrays support a variety of EKMs certified by FIPS 140-2. By securely producing, safeguarding, serving, regulating, and auditing encryption keys on a separate server, EKMs provide a full security solution for integrating and automating an organization's encryption policies. FIPS-certified drives and a FIPS-compliant EKM are both required for FIPS-compliant DAR encryption on the array. Use of FIPS-certified drives with the onboard LKM is not compliant with FIPS 140-2 standards.

Full conversion between key manager types is possible. The array can transition from LKM to EKM, EKM to LKM, or EKM to another EKM (through intermediate transition to LKM), without halting the DAR encryption process.

The HPE Alletra Storage MP B10000 data-at-rest encryption technical white paper covers this topic in greater detail.

Note
For more information about EKMs supported by HPE Alletra Storage MP B10000 arrays, visit HPE SPOCK.

Syslog

HPE Alletra Storage MP B10000 arrays support sending log messages to two types of syslog servers. The first target is a general syslog server that receives messages related to the operation and use of the array. The second is a secure syslog server, to which messages associated with user login actions and changes to the system settings, such as encryption management, are sent. The secure syslog server can be a valuable early warning system providing real-time alerts of potentially malicious access attempts to the array.

Secure syslog messages are always sent using TLS to ensure the data being sent is encrypted.

SNMP

Simple Network Management Protocol (SNMP) managers are systems that can collect, store, view, and manage event messages and alerts from devices on a network. In normal operation, an SNMP manager polls the devices for messages. However, when a device identifies important events, it can push an alert (also known as an SNMP trap) to the SNMP manager without waiting to be polled.

HPE Alletra Storage MP B10000 supports SNMP v3, which provides confidentiality by encrypting the data within SNMP packets, integrity through cryptographic hashing to help ensure data has not been tampered with, and authentication to help ensure that the data is from a valid source. This is a major improvement from SNMP v1 and v2/c, where authentication consisted of a password, or community string, sent in clear text between a manager and network device. HPE Alletra Storage MP B10000 uses AES-128 encryption and HMAC-SHA-96 hashing algorithms for SNMP v3.

FIPS mode

FIPS mode is a setting that requires the use of NIST-validated cryptographic modules for communication between the array and external systems. When enabled on HPE Alletra Storage MP B10000 arrays, it helps ensure that only FIPS-compliant modules for encrypted communications are in use—including specific disk types and algorithms in software libraries—while disabling components not compliant with FIPS.

Examples of storage system communication interfaces that use FIPS mode include UI to server, SMI-S CIM, CLI, EKM, LDAP, QW, SNMP, SSH, SYSLOG, VASA, WSAPI and RDA.

Common Criteria (CC) mode

CC mode enforces the use of only Common Criteria approved cipher suites and hashing algorithms for LDAP, SSH and syslog services. CC mode also enforces the use of strict X.509 certificate verification when connecting to a remote security syslog server. CC mode is disabled by default and will reset all SSH sessions when enabled. It is advised to review the information in the following section to ensure compatibility, so communication is not disrupted when enabling CC mode.

Supported cipher suites and encryption algorithms

HPE Alletra Storage MP B10000 supports a range of modern cipher suites for secure communication using Transport Layer Security (TLS) and Secure Shell (SSH). Tables 1 and 2 show the cipher suites supported for TLS and SSH communication.

Table 1. Supported TLS cipher suites

Service	Cipher Suites	Elliptic Curve Groups
WSAPI/CLI/VASA/EKM/QW/Syslog	• TLS AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384	• x25519 (disabled by CC mode) • secp256r1 • x448 (disabled by CC mode) • secp512r1 • secp384r1 • ffdhe2048 • ffdhe3072 • ffdhe4096 • ffdhe6144 • ffdhe8192
LDAP	• TLS_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• x25519 (disabled by CC mode) • secp256r1

	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256	• x448 (disabled by CC mode) • secp512r1 • secp384r1 • ffdhe2048 • ffdhe3072 • ffdhe4096 • ffdhe6144 • ffdhe8192

Table 2. Supported SSH cipher suites

Ciphers	MAC	Key Exchange Algorithms
• aes256-gcm@openssh.com • aes128-gcm@openssh.com • aes128-ctr • aes192-ctr • aes256-ctr	• hmac-sha2-512-etm@openssh.com • hmac-sha2-256-etm@openssh.com • hmac-sha2-512 • hmac-sha2-256	• diffie-hellman-group-exchange-sha256 (disabled by CC mode) • diffie-hellman-group14-sha1* • diffie-hellman-group14-sha256* • diffie-hellman-group16-sha512* • diffie-hellman-group18-sha512* • ecdh-sha2-nistp256* • ecdh-sha2-nistp384* • ecdh-sha2-nistp512* * (disabled by default, enabled by CC mode)

User access control

HPE Alletra Storage MP B10000 supports robust access control mechanisms such as multifactor authentication (MFA) using a DoD Common Access Card, role-based access control (RBAC), LDAP, and secure shell (SSH).

Multifactor authentication (MFA)

HPE Alletra Storage MP B10000 arrays uses MFA to validate the user by using a U.S. Department of Defense (DoD) Common Access Card (CAC) as a second method of authentication. MFA requires the user to have a PIN and a one-time password to prevent malicious agents from compromising a user account to access secure information—even if credentials have been exposed.

Role-based access control (RBAC)

Role-based access control restricts access to the array based on the user's role within the organization. When creating a user account, you can assign one of the roles listed in Table 1.

Table 3. User roles

Role	Description
Super	Rights are granted for all actions and operations.
Service	Rights are limited to actions and operations that are required to service the arrays. This role allows limited access to user information and user group resources.
Security admin	Rights are granted to create and remove user accounts, except user accounts that have the super role.
Edit	Rights are granted to most actions and operations (for example, creating, editing, and deleting storage volumes).
Create	Rights are limited to creating items (for example, creating storage volumes).
Browse	Rights are limited to read-only access (for example, viewing storage volume information).
Basic edit	Rights are like the edit role but are more restrictive for deleting objects.

LDAP

Users can also be authenticated through Lightweight Directory Access Protocol (LDAP). LDAP servers typically provide a directory for sharing details about objects in network, such as user credentials, enabling different applications and services to authenticate users. The customer can use supported LDAP servers to authenticate credentials requesting access to an array by non-local users. If the customer's environment uses LDAP for authentication and authorization, an LDAP configuration can be specified in the HPE Alletra Storage MP B10000 array.

HPE Alletra Storage MP B10000 supports the following LDAP servers:

- Microsoft Active Directory
- OpenLDAP
- Red Hat® Directory Server

Secure shell (SSH)

Most host operating systems supported by HPE Alletra Storage MP B10000 include an SSH client that can be used to access the HPE Alletra Storage MP B10000 CLI. The exception is Windows, which requires installing an SSH client. Using SSH requires no additional installation or setup of the HPE Alletra Storage MP B10000 CLI.

The benefits of SSH access include:

- **Security**:
  - Encryption: SSH uses strong encryption to secure information exchanged between the client and the server.
  - Server authentication: SSH uses SSH key pairs for server authentication. SSH key pairs are asymmetric encryption keys and contain a public and a private key in each pair. The public key can be stored on the client side, enabling the SSH client to compare the key hash presented by the server before granting access.
  - User authentication: SSH supports the use of secure password and SSH key pairs for user authentication.
- **Data integrity:** SSH uses integrity checking to verify that data is not altered during transmission from sender to receiver.
- **Compatibility:** SSH removes compatibility issues between client and server if no HPE Alletra Storage MP B10000 CLI client is installed.

Password length and complexity

Modern GPUs have increased the speed at which malicious actors can crack weak passwords. Increasing the length and complexity of passwords dramatically increases the work effort required to achieve this, improving the chance of detecting an intrusion event. HPE Alletra Storage MP B10000 supports password lengths of up to 32 characters with characters classes of lower-case, upper-case, numerical and special characters. Administrators can define a minimum password length and minimum password complexity (enforcing 1-, 2-, 3- or 4-character classes that must be used), ensuring that all newly created passwords meet required security standards. HPE recommends the minimum password length to be configured to 16 or more if multiple character classes are being enforced.

Unsuccessful login attempts

Multiple failed login attempts either to the CLI or GUI will result in the user being locked out for a configurable period and an alert being generated. During the lockout period any attempt by the locked user to authenticate, even with a valid password, will be denied. The

maximum number of login attempts before lockout can be configured along with the duration of the lockout period, setting the lockout duration to 0 will result in a user being locked out indefinitely, until an administrator unlocks the account.

Array certificates

Digital certificates signed by a certificate authority (CA) play a key role in securing communication between nodes on a network providing authentication, integrity, trust, and form the backbone for secure transmission of symmetric keys for encrypted communication to ensure data confidentiality. HPE Alletra Storage MP B10000 provides the ability to install certificates for several array functions that require communication with an external network entity, for example communicating with an external key manager, directory service or secure syslog server.

Whilst self-signed certificates can be generated on the array for these array functions it is advisable to generate a certificate signing request (CSR) and submit that to a CA to produce a trusted, signed certificate. As well as not being issued by a trusted CA, self-signed certificates are not scalable or centrally manageable leading to increased management complexity and increased risk of a malicious actor posing as a legitimate entity.

HPE Alletra Storage MP B10000 array support x.509 certificates with RSA keys of 2048-,3072-, and 4096-bits with SHA2 signature algorithms.

X.509 Certificate validation

HPE Alletra Storage MP B10000 OS uses Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking to determine if stored certificates are valid and automatically removes them if they are confirmed to be revoked as they must not be trusted. This check is performed when a certificate is imported to the system, and again every 12 hours. If the OCSP Responder or CRL endpoint cannot be contacted no action is performed, and if the certificate imported contains no OCSP or CRL information the check will not occur.

Syslog and LDAP services perform certificate validation for each connection, during this process the entire peer chain is checked using either OSCP or CRL depending on which fields the certificate contains. If any certificate in the peer chain is found to be revoked the TLS connection will be terminated and an alert generated. If a revocation check is unsuccessful, the connection is established but an alert is generated informing the administrator that the revocation check could not be completed.

NTP authentication

Network Time Protocol (NTP) synchronizes networks to a single time source, this is essential for many system applications such as email, certificate revocation checking and generating log file time stamp information. NTP can be an intrusion point on a network whereby a malicious actor may spoof an NTP server to provide incorrect time information to a time receiver, opening the doors for expired cryptographic keys to be accepted as valid, or to modify time stamps on log files to cover their tracks. NTP authentication allows an NTP client to verify the authenticity of an NTP server using pre-shared cryptographic keys. This pre-shared key is used to append a cryptographic signature to each network packet so the NTP client can be sure that the packet it receives originated from the expected NTP server.

iSCSI authentication

Challenge-Handshake Authentication Protocol (CHAP) for iSCSI is supported by HPE Alletra Storage MP B10000. CHAP uses a challenge-response mechanism to authenticate iSCSI initiators. A shared “secret”, or password, allows the system to verify that the iSCSI initiator is who it claims to be and is authorized to access the data. CHAP is not supported for iSCSI discovery sessions, only for normal sessions.

NVMe/TCP authentication

The B10000 supports Diffie-Hellman Hashed-Message Authentication Code Challenge-Handshake Authentication Protocol (DH-HMAC-CHAP) for NVMe over TCP connected hosts. DH-HMAC-CHAP is a key based authentication and key management protocol and forms an enhanced version of CHAP used by iSCSI and can provide unidirectional authentication where the target authenticates the host or bidirectional authentication where the target and initiator authenticate each other.

Secure inter-node and inter-enclosure communication

Due to its disaggregated architecture a HPE Alletra Storage MP B10000 system can consist of multiple controller node enclosures and multiple expansions shelves. All communication between nodes and/or expansion shelves uses SSH, authenticating via SSH key. During installation the initial SSH keys are changed from the default and the new key is transferred to all the controller nodes and expansion shelf nodes to maintain secure connectivity.

HPE Alletra Storage MP B10230 and B10240 models connect to the HPE Alletra Storage MP expansion shelves via two 32-port 100GbE switches. All communication between the nodes and the switches is via REST APIs using secure, randomly generated, passwords which are established during initial configuration in the supply chain.

Ransomware detection

HPE Alletra Storage MP B10000 systems are designed to detect data encryption that may be the result of a ransomware attack. Data written to a volume is sampled and examined by independent algorithms to detect encryption activity and will alert users if the change in data is suspicious. If a detection alert is raised, the involved volume is flagged as degraded and an immutable, read-only snapshot of the volume is generated. Users are notified via syslog, email and DSCC informing them of the affected volume and that an alert snapshot has been generated, these alerts are also sent to HPE Support via Call-Home. Normal volume operations are not suspended when an alert is raised, and I/O continues as normal.

Data encryption detection is not anti-virus style malware scanning and is not capable of detecting ransomware activity before encryption has started. It should be used in conjunction with (not as a replacement for) SIEM/XDR/SOAR systems, array hardening, and data protection with Virtual Lock snapshots and other backup solutions. The alert snapshot generated will contain data that caused the detection alert so is not intended to be used as a recovery snapshot, but for analysis to determine if the alert raised is due to genuine ransomware activity or legitimate encryption activity.

The HPE Alletra Storage MP B10000: cyber resilience with data adaptive ransomware detection technical white paper covers this solution in more detail.

Array hardening

An administrator's hardening guide is available which provides detailed instructions and recommendations for strengthening the security of a B10000 array. It outlines specific configurations and best practices to prevent unauthorized access, minimize vulnerabilities and reduce the risk of cyber-attacks. The HPE Alletra Storage MP B10000 administrator's hardening guide has been produced in conjunction with the Department of Defense Security Technical Implementation Guides which currently in development.

External connections

In addition to the internal security features, HPE Alletra Storage MP B10000 arrays can use other features to further protect data in communications with external or remote components and services.

HPE Alletra Storage MP B10000 replication software

The HPE Alletra Storage MP B10000 replication software brings a rich set of features that can be used to design disaster-tolerant and cost-effective solutions that address disaster recovery challenges. It is a uniquely easy, efficient, and flexible replication technology that enables the customer to protect and share data from any application.

Implemented over an IP network or Fibre Channel SAN, the administrator may flexibly choose one of three data replication modes to design a solution that meets the workload's requirements for recovery point objectives (RPOs) and recovery time objectives (RTOs):

- Synchronous
- Asynchronous periodic (for asynchronous replication)
- Active Peer Persistence

Synchronous replication

Synchronous replication provides zero data loss in the event of failure, offering the ultimate RPO—but it can impact host performance. Because spinning media solutions measure performance in tens of milliseconds, creating an exact copy of data over an extended distance adds some latency, but it generally meets service-level agreements (SLAs). All-flash systems, such as HPE Alletra Storage MP B10000 arrays, are more sensitive to latency overheads because performance is measured in microseconds—so any overhead measured in milliseconds can significantly increase latency. The overhead of replicating every write request over an IP link might have this impact, considering the round trip.

Asynchronous periodic replication

Based on snapshots and delta resyncs, asynchronous periodic replication has minimal impact on host performance. It does require a compromise because RPOs can be only as low as 30 seconds, not just a few seconds or milliseconds. This might be suitable for applications for which RPOs up to 30 seconds are acceptable, but data compliance and business needs can often require lower RPOs. The periodic asynchronous replication mode can be configured with a sync interval as low as 15 seconds for a best-case RPO of 30 seconds.

Changed data within an HPE Alletra Storage MP B10000 Remote Copy volume group is transferred only once between synchronization intervals—no matter how many times it might have changed. In addition, efficiencies in the initial copy creation of the target volumes that do not require replication of zero data across the replication network, regardless of target volume type (thin or reduce), result in faster initial synchronization and better network utilization.

Active Peer Persistence

The HPE Alletra Storage MP B10000 Active Peer Persistence software is layered on top of synchronous replication and enables the block storage systems located within a metropolitan distance to act as peers to each other to deliver a high-availability, transparent failover solution for the connected clusters running VMware vSphere®, Windows, and Microsoft Hyper-V, Red Hat Enterprise Linux®, SUSE Linux Enterprise Server, HP-UX, or AIX. HPE Alletra Storage MP B10000 Active Peer Persistence allows an array-level, high-availability solution between two sites or data centers, with failover and failback completely transparent to the hosts and applications. Unlike traditional disaster recovery models in which the hosts (and applications) must be restarted upon failover, HPE Alletra Storage MP B10000 Active Peer Persistence enables hosts to remain online, serving their business applications—even when the workload I/O migrates transparently from the primary array to the secondary array—with zero downtime.

Note
The HPE Active Peer Persistence technical white paper covers this topic in greater detail.

HPE GreenLake

The HPE GreenLake cloud offers a common set of cloud services that enable a consistent, cloud-qualified customer experience. The HPE GreenLake is designed to combine the cloud's agility with the governance, compliance, and visibility of the hybrid cloud model.

Key features of the HPE GreenLake make it easy for new cloud users to get started while offering powerful capabilities for advanced users:

- Global data management for streamlined configuration and deployment of devices
- Support for device management, which enables customers to provision and manage multiple devices that have similar configuration requirements with less administrative overhead
- A secure cloud-based platform
- Rich API that enables customers to implement data management functionality

Data Services Cloud Console

Data Services Cloud Console (DSCC) is a secure cloud application, deployed on the HPE GreenLake, which provides a control plane for simplifying data infrastructure management and delivering data services across edge-to-cloud environments. This enables a unified management experience for the customer's cloud-enabled arrays.

Security is at the heart of the design of DSCC. Data written to the on-premises array, and to on-premises components such as virtual machines, is not accessible to DSCC. The array establishes a TLS tunnel to DSCC through its management network, helping to ensure that its data is never exposed to the internet. The secure tunnel is always initiated by the array, never from DSCC. This guarantees there is no need for any inbound traffic to the array.

Note
For more information about Data Services Cloud Console security, refer to the DSCC security guide.

Read-only mode

The B10000 array can be configured to restrict DSCC access to read-only, allowing users with access to DSCC to view the array settings but not modify them, by default this is disabled but enabling this feature restricts the DSCC privileges on the array to a browse role.

Detecting security updates

HPE Alletra Storage MP B10000 arrays are regularly scanned during the product development stage to identify any vulnerabilities. HPE also engages with third-party security scan organizations for activities, such as penetration testing, to help ensure that any identified vulnerabilities are addressed. Because vulnerabilities keep emerging even after products are released, HPE has processes in place to assess these vulnerabilities and address them as needed.

HPE Alletra Storage MP B10000 helps mitigate those threats by using upgrades. It changes the architecture by which fixes for CVEs can be pushed quickly to the HPE Alletra Storage MP B10000 OS. The administrator does not have to wait for a new kernel build of the OS to address vulnerabilities. With HPE Alletra Storage MP B10000, HPE creates an update package and pushes it to the array. Administrators can apply the update during a scheduled maintenance window or immediately upon arrival without disrupting the user environment. This approach keeps the array up to date to guard against the latest known CVEs.

HPE Remote Device Access

HPE Remote Device Access (RDA) is a remote connectivity solution for devices on client networks that enables remote service delivery, support automation, real-time monitoring, and quality feedback. To enable secure connectivity between HPE and HPE Alletra Storage MP B10000, RDA employs forward and reverse proxy technology.

RDA includes two features that ensure safe data transfer:

- **Authenticated endpoint identification**—Providing a secure method for HPE support engineers to find customer devices and connect them securely.
- **Layered security protocol with a meet-in-middle-architecture**—Providing a two-point authority, allowing user access control at the HPE midway servers, and enabling Customer Access Services for the HPE Alletra Storage MP B10000 arrays. Customer Access Services can enable HPE remote support, data transfer of device telemetry to HPE, and diagnostic or update packages from HPE to the array.

RDA capabilities help restrict access to the remote desktop port by guaranteeing that the data communicated is delivered only to approved customers and that ransomware actors or unauthorized outsiders do not have access to the remote desktop.

Recovery

This section discusses the capabilities of HPE Alletra Storage MP B10000 arrays during the recovery of a ransomware attack by using their enhanced features, such as Virtual Copy and immutable snapshots. For more information about ransomware recovery, refer to the Ransomware data recovery technical white paper.

Virtual Copy

Virtual Copy is the HPE Alletra Storage MP B10000 snapshot implementation used to provide a point-in-time Virtual Copy of a virtual volume (VV). It helps ensure that the original data can always be obtained because it provides a point-in-time copy of the volume in case data is inadvertently deleted. Virtual Copy is implemented by using a redirect-on-write (RoW) mechanism that eliminates any performance impact to host I/O by writing changed data to a new array, avoiding the copy operations necessary with copy-on-write (CoW) implementations.

Virtual copies are thin and reservationless, with only one copy of a changed block. Thanks to efficient metadata handling, the administrator can configure thousands of read-only and read-write snapshots. Flexible management allows any snapshot to be promoted without destroying any other snapshots.

Virtual Lock immutable snapshots

Immutable snapshots are snapshots that cannot be written to or deleted. The snapshot is initially constructed as a read-only snapshot with a predetermined expiration period (Virtual Lock). Hewlett Packard Enterprise recommends that a snapshot be inspected for infection and, if it is determined to be clean, that it be locked in a “clean room.” If a ransomware attacker uses stolen administrative credentials and deletes all backups, immutable snapshots (Virtual Lock snapshots) from the clean room can be restored because they are free from malware.

Note

For more information, read the Ransomware data recovery architectures technical white paper.

HPE StoreOnce

HPE StoreOnce is a purpose-built backup appliance (or virtual machine) that includes HPE StoreOnce Catalyst stores. These stores effectively isolate critical data where attackers cannot harm it without resorting to direct physical interactions that would ultimately destroy some or all of the hardware itself. Even if malware achieves physical destruction at a single location, the more advanced implementation of HPE StoreOnce Catalyst stores (distributed implementation) protects mission-critical data by effectively isolating it from traditional lines of communication and command sets leveraged by ransomware attackers. HPE has "hidden" the HPE StoreOnce Catalyst store from attackers in plain sight, behind an application programming interface (API) that both enhances and simplifies the process of backing up and deduplicating data, while making it practically impossible for ransomware to attack it directly.

HPE StoreOnce Catalyst stores do not prevent the rest of the environment from being compromised by malware, but they do protect stored mission-critical data from being targeted or affected. Ransomware cannot encrypt what it cannot see, and because the HPE StoreOnce Catalyst stores do not use standard operating system command instructions for their operations, malware cannot become active in them. HPE StoreOnce Catalyst efficiently backs up and restores data by using a tamperproof method. HPE StoreOnce Catalyst—initially designed for use as a disk-based solution and now extended to the cloud—can leverage deduplication, compression, encryption, and data isolation for backup and archiving processes. HPE StoreOnce Catalyst prevents ransomware from accessing data on the HPE StoreOnce appliance, ensuring data integrity.

HPE Zerto Cyber Resilience Vault

The HPE Zerto Cyber Resilience Vault is a reference architecture based on HPE Alletra, HPE ProLiant, HPE Aruba Networking and HPE Zerto Software and consists of three core pillars utilizing a decentralized Zero Trust architecture to achieve rapid air-gapped recovery in the event of a ransomware incident.

- **Replicate and detect:** Streaming, near-synchronous data replication protects every production write in real time and immediately detects and alerts on any suspicious anomalies. Continuous data protection (CDP) in HPE Zerto is agentless, so there is nothing inside a protected VM that can be disabled or hijacked by malware.
- **Isolate and lock:** The vault itself also includes HPE ProLiant and HPE Alletra storage. This separated vault is physically air-gapped with no access to the internet or production network. It stores immutable data copies on secure, high-performance, FIPS-validated hardware.
- **Test and recover:** Easily identify clean restore points, then quickly recover entire multi-VM apps onto high performance storage—all while maintaining cross-VM consistency, even with thousands of VMs. HPE Zerto features a unique, battle-tested journal that unlocks RTOs of minutes or hours, not days or weeks.

Summary

The security features available for HPE Alletra Storage MP B10000 arrays provide multiple routes to protect workloads against data breaches and malware attacks, mitigating damage and offering recovery options from such attacks. HPE Alletra Storage MP B10000 product architecture also includes features that enable organizations to meet U.S. federal security and other regulatory compliance standards, such as those required during security audits. These certifications and regulations not only support compliance, but also include benefits, such as the hardening of the array and the use of strong cryptographic algorithms to keep data secure. The security features covered in this document enable administrators to customize internal and external configurations and services, providing options to satisfy all levels of data protection, high availability, and security requirements. For examples of how to implement many of the features discussed in this document see the HPE Alletra Storage MP B10000 Administrators hardening guide.

Additional resources

HPE Alletra Storage MP B10000 architecture
hpe.com/psnow/doc/a50008302enw?from=app&section=search&isFutureVersion=true

Data Services Cloud Console security guide
hpe.com/psnow/doc/a00113337enw?from=app&section=search&isFutureVersion=true

HPE Alletra Storage MP B10000 administrators hardening guide
hpe.com/psnow/doc/a00146015enw

HPE Alletra Storage MP B10000 data-at-rest encryption technical white paper
hpe.com/psnow/doc/a00136828enw?from=app&section=search&isFutureVersion=true

HPE Alletra Storage MP B10000: cyber resilience with data adaptive ransomware detection
hpe.com/psnow/doc/a00147482eew

HPE Active Peer Persistence technical white paper
hpe.com/psnow/doc/a00115612enw?from=app&section=search&isFutureVersion=true

Ransomware data recovery architectures
hpe.com/psnow/doc/a00119614enw?from=app&section=search&isFutureVersion=true

HPE Single Point of Connectivity Knowledge (SPOCK)—requires registration
h20272.www2.hpe.com/SPOCK/index.aspx

Protecting data from ransomware with HPE StoreOnce Catalyst
hpe.com/psnow/doc/a00042003enw?from=app&section=search&isFutureVersion=true

HPE Zerto Cyber Resilience Vault
zerto.com/solutions/use-cases/cyber-recovery/cyber-resilience-vault/

Learn more at

HPE.com/storage

Visit HPE.com

Chat now (sales)

a00138815ENW, Rev. 3

Hewlett Packard Enterprise