Technical white paper

HPE Alletra Storage MP B10000

Administrators hardening guide

Contents

Executive summary

In today's rapidly evolving digital landscape, the integrity and security of storage arrays—critical components of any organization's IT infrastructure—are under increasing threat. Cybercriminals are becoming more sophisticated, targeting storage systems with ransomware, data breaches, and other malicious activities that can result in significant financial and reputational damage.

As organizations continue to adopt new technologies and expand their digital footprints, the potential attack surface grows, making storage arrays a prime target for adversaries seeking to exploit vulnerabilities. These systems often contain vast amounts of sensitive and proprietary information, making them a high-value target for attackers.

The threat landscape is typically characterized by:

- **Ransomware attacks:** Cybercriminals often target storage arrays to encrypt large volumes of data, demanding ransom payments to restore access.
- **Data breaches:** Unauthorized access to storage systems can lead to the exposure of confidential data, leading to compliance violations and loss of trust.
- **Advanced persistent threats (APTs):** Sophisticated attackers may establish a foothold within storage networks, silently exfiltrating data over time or corrupting critical information.
- **Insider threats:** Employees or contractors with malicious intent can exploit access to storage systems, causing significant harm to the organization.

Securing storage arrays is essential for the following reasons:

- **Data integrity:** Ensuring that the data stored is accurate, complete, and protected from unauthorized alteration or destruction.
- **Business continuity:** Protecting storage arrays from attacks helps maintain uptime and ensures that critical business operations can continue without disruption.
- **Regulatory compliance:** Many industries are subject to stringent data protection regulations (such as GDPR, HIPAA, or CCPA). Ensuring that storage arrays are secure is crucial to maintaining compliance and avoiding costly penalties.
- **Reputation management:** Protecting customer and business data from breaches helps maintain trust and avoids the negative press associated with data incidents.

This guide provides best practices for hardening HPE Alletra Storage MP B10000 systems, helping organizations to proactively protect their critical data assets from the evolving threats of the digital age. By implementing the recommended security measures, organizations can mitigate risks, safeguard their data, and ensure long-term operational resilience.

Target audience

This document is designed to be a reference guide for storage array administrators, security officers, security architects and anyone else wishing to learn more about how HPE Alletra Storage MP B10000 arrays can be secured effectively. It is assumed that the reader has prior knowledge and experience of configuring and managing HPE Storage arrays through the command line interface.

Document purpose

This document discusses the features that can be hardened from a default configuration and offers a set of security best practices based on the forthcoming U.S. Department of Defense (DoD) Security Requirements Guide (SRG), considering both the current threat environment and capabilities of the product. The document is broken down into different security domains such as **authentication and authorization, secure communication,** and **compliance and reporting.** Each security domain features the functions that administrators may wish to harden and provides examples of how these functions can be secured. Not all sections may be applicable to each environment, but it is recommended to read the whole document before determining how to implement any changes that may be required by organizational and regulatory requirements. This document does not cover data protection settings such as protection schedules, ransomware detection, replication, or virtual lock and is focused on securing the storage array against external threat actors.

Authentication and authorization

Authentication and authorization are two extremely important processes that system administrators use to protect IT systems, and the information contained with them. Authentication verifies the identity of a user or service, and authorization deals with the access rights said user or service has on the system.

Minimum password length

Modern GPUs have increased the speed at which attackers can crack weak passwords. By increasing the length and complexity of the password the work effort required by attackers increases drastically, improving the chance of detecting an intrusion event. HPE Alletra Storage MP B10000 OS supports password lengths for local users of up to 32 characters.

```
cli% showsys -d
----------------------General-----------------------
System Name                 :               5UH8359406
System Model                :   HPE Alletra Storage MP
Serial Number               :               5UH8359406
Product Number              :                   S0B84A
System ID                   :                  0x7EE49
Number of Nodes             :                        2
Master Node                 :                        0
Nodes Online                :                      0,1
Nodes in Cluster            :                      0,1
Chunklet Size (MiB)         :                     1024
Minimum PW length           :                        8
Minimum PW character classes:                        1
Subscription Status         :               Subscribed

cli% setsys MinimumPWLength 24

cli% showsys -d
----------------------General-----------------------
System Name                 :               5UH8359406
System Model                :   HPE Alletra Storage MP
Serial Number               :               5UH8359406
Product Number              :                   S0B84A
System ID                   :                  0x7EE49
Number of Nodes             :                        2
Master Node                 :                        0
Nodes Online                :                      0,1
Nodes in Cluster            :                      0,1
Chunklet Size (MiB)         :                     1024
Minimum PW length           :                       24
Minimum PW character classes:                        1
Subscription Status         :               Subscribed
```

Minimum password complexity

A minimum level of password complexity can be enforced for newly created passwords. With no check in place users can pick easy to guess passwords that may leave a system vulnerable to brute force attacks. The B10000 provides storage administrators with the ability to specify the minimum number of character classes (a value between 1 and 4) that must be present in newly created passwords. These character classes are:

– Upper case letters

– Lower case letters

– Numbers

– Special characters

```
cli% showsys -d
----------------------General-----------------------
System Name                 :               5UH8359406
System Model                :   HPE Alletra Storage MP
Serial Number               :               5UH8359406
Product Number              :                   S0B84A
System ID                   :                 0x7EE49
Number of Nodes             :                      2
Master Node                 :                      0
Nodes Online                :                    0,1
Nodes in Cluster            :                    0,1
Chunklet Size (MiB)         :                   1024
Minimum PW length           :                     24
Minimum PW character classes:                      1
Subscription Status         :               Subscribed

cli% setsys MinimumPWCharacterClasses 4

cli% showsys -d
----------------------General-----------------------
System Name                 :               5UH8359406
System Model                :   HPE Alletra Storage MP
Serial Number               :               5UH8359406
Product Number              :                   S0B84A
System ID                   :                 0x7EE49
Number of Nodes             :                      2
Master Node                 :                      0
Nodes Online                :                    0,1
Nodes in Cluster            :                    0,1
Chunklet Size (MiB)         :                   1024
Minimum PW length           :                     24
Minimum PW character classes:                      4
Subscription Status         :               Subscribed
```

When attempting to change a password or create a new user with a password that does not comply with the minimum complexity requirements an error will be shown.

```
cli% createuser -c test99 user1 all browse
Unsuitable password: not enough different characters or classes

cli% createuser -c 'TeST!-#99' user1 all browse
User created

cli% setpassword -u user1
New password for user user1: # test99
Re-type new password:

Unsuitable password: not enough different characters or classes
```

Failed login attempts

Multiple failed login attempts 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. Certain service user account such as hpesupport are not included in this.

To configure the maximum number of allowed login attempts and the lockout duration use the following commands:

Enable the feature:

```
cli% controlsecurity maxloginattempts enable
```

Disable the feature:

```
cli% controlsecurity maxloginattempts disable
```

Show the status of the feature:

```
cli% controlsecurity maxloginattempts status
maxloginattempts in enabled
```

Sets the maximum number of failed login attempts:

```
cli% controlsecurity maxlogincount set <1-15>
```

Show the current maximum number of failed login attempts:

```
cli% controlsecurity maxlogincount show
Current maximum login count in the system: 3
```

Set the duration a user is locked out for in minutes (setting to 0 results in an indefinite lockout):

```
cli% controlsecurity lockout_duration set <0-1440>
```

Show the configured lockout duration:

```
cli% controlsecurity lockout_duration show
Current lockout duration value in the system: 15 minutes
```

Users that have been locked will remain locked until the lockout duration has elapsed, or until an account with sufficient privileges unlocks it:

To unlock a user:

```
cli% controlsecurity user unlock <user_name>
User <user_name> is successfully unlocked
```

To unlock all locked users

```
cli% controlsecurity user unlock -a
```

```
Found 2 user(s), unlocked 1 user(s), skipped 1 user(s)
```

To display the login information of all users, or a specified user

```
cli% controlsecurity user show [<user_name>]

UserName     LastLogin           CurrFailed Status
admin        2025-04-30 09:28:52 UTC    0 Unlocked
user         2025-04-30 09:28:52 UTC    5 Locked
-------------------------------------------------------
            2 total
```

Directory services

Using directory services such as Microsoft Active Directory, OpenLDAP, or Red Hat® Directory Service provides significant benefits over local user accounts such as centralized management of user accounts and better security through global password policies and easier user provisioning and deprovisioning. Directory services allow for easier management of user authorization by providing the ability to map specific user directories to array roles. Lightweight directory access protocol (LDAP) communications can be secured using LDAPS (LDAP over SSL) or StartTLS; however, LDAPS is now considered deprecated, and it is best practice to secure LDAP communication using StartTLS.

Microsoft Active Directory

An example configuration to connect to Microsoft Active Directory is shown in the following. Many of the connection properties and authentication parameters are shown but exact configuration will vary by environment. For a full reference of all available configuration options, see the HPE Alletra Storage MP B10000 CLI reference guide.

```
cli% showauthparam
no authentication parameters listed

cli% setauthparam -f ldap-type MSAD
cli% setauthparam -f ldap-server 16.172.72.91
cli% setauthparam -f ldap-server-hn lr4-gcdc-01.lr4-storage.net
cli% setauthparam -f binding simple
cli% setauthparam -f ldap-StartTLS require
cli% setauthparam -f ldap-ssl 0
cli% setauthparam -f ldap-port 389
cli% setauthparam -f kerberos-realm LR4-STORAGE.NET
cli% setauthparam -f kerberos-server 16.172.72.91
cli% setauthparam -f user-dn-base "CN=Users,DC=lr4-storage,DC=net"
cli% setauthparam -f user-attr LR4-STORAGE\\

cli% setauthparam -f account-obj user
cli% setauthparam -f account-name-attr sAMAccountName
cli% setauthparam -f accounts-dn “OU=test,DC=lr4-storage,DC=net”
cli% setauthparam -f memberof-attr memberOf

cli% setauthparam -f super-map "CN=grp-test-super-global,OU=test,DC=lr4-storage,DC=net"
cli% setauthparam -f edit-map "CN=grp-test-edit-global,OU=test,DC=lr4-storage,DC=net"
cli% setauthparam -f browse-map "CN=grp-test-browse-global,OU=test,DC=lr4-storage,DC=net"
cli% setauthparam -f service-map "CN=grp-test-service-global,OU=test,DC=lr4-storage,DC=net "
```

Example showauthparam command after configuration:

```
cli% showauthparam
ldap-type            MSAD
kerberos-realm       LR4-STORAGE.NET
kerberos-server          16.172.72.91
ldap-server-hn       lr4-gcdc-01.lr4-storage.net
ldap-server          16.172.72.91
ldap-ssl             0
ldap-port            389
ldap-StartTLS        require
binding              simple
accounts-dn          OU=test,DC=lr4-storage,DC=net
super-map            CN=grp-test-super-global,OU=test,DC=lr4-storage,DC=net
edit-map             CN=grp-test-edit-global,OU= test,DC=lr4-storage,DC=net
browse-map           CN=grp-test-browse-global,OU= test,DC=lr4-storage,DC=net
service-map          CN=grp-test-service-global,OU= test,DC=lr4-storage,DC=net
audit-map            CN=grp-test-audit-global,OU= test,DC=lr4-storage,DC=net
ldap-ssl-cacert:
-----BEGIN CERTIFICATE-----
MIIFmDCCA4CgAwIBAgIQEz6/R4aRzr1CJGW2OIlczTANBgkqhkiG9w0BAQsFADBL
MRMwEQYKCZImiZPyLGQBGRYDbmV0MRswGQYKCZImiZPyLGQBGRYLbHI0LXN0b3Jh
Z2UxFzAVBgNVBAMTDmxyNC1zdG9yYWdlLUNBMB4XDTIyMDUzMTE3Mjg1MFoXDTMy
MDUzMTE3Mzg0NFowSzETMBEGCgmSJomT8ixkARkWA25ldDEbMBkGCgmSJomT8ixk
ARkWC2xyNC1zdG9yYWdlMRcwFQYDVQQDEw5scjQtc3RvcmFnZS1DQTCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAL4rFacYmmrmLrjlkkCUYBonZ8AGf/Xu
KXAPufa7ta+B4wk+wPmKckT3vaIUeG6yf8Q5KmvQq3cPfnsZZghobkl/CUpPXKI1
BoBXHXocrsdxNROnr/hN1hTcDCZRcz8ww8SrnkoFLFkK48qHKM9NkKsDvIOZyElG
yMGOyLeCOOQ5vyyQBc2b/FmHyyJFUjrKryO133G3xFTOtsCf85kTizSpwrh1l7zc
0/114iATNlRO5ZlU987rmWrOaOApCMGplUoZU3lXBVTh4gfZNURXWJUjBN8SwHHo
fNJeTmxY0IcKLEWZIZS6wwdtKvcTmoD35qMta5D76fKGM+YgEIvCzUT4pRC3tfJo
68ludbt+1D0Dd/C08fCgB9dbvJ9ZNJlJhfyeGjUe3cIEDkmvz9KsGDAl4CwUWAJj
YR98HCi1swQjSGYNluojQIXGHJOhqAx1HLwmFfYww1LVBKlzkdcCVQMLV4T1D0Ne
idVcMqD7k6BuCOGMFUBElM6Mz5mOOUJ9OafLL1bXiGeN50SaHfqJRuXONJOAsH4c
QWgZKJpdECZARuEtCR4zNzP8SMYRPmw7npxwfbqYIUvdL5jIA+q9FSEq54Wmpc6u
7BCBboypsUAcANzgbBA5Ug4nnTGhzSY+BlZ99xjcPqjaKQAX8FKfakYKqJwOHVVG
+l4rFouquOXNAgMBAAGjeDB2MAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/

qxbvezU1yLDlSmFiHWxnLW6oNUGW3tBOUdykrFRMTm/tfmcKtHiODXfO8ag=
-----END CERTIFICATE-----
```

If ldap-StartTLS is set to **required**, it is also necessary to import the LDAP server root certificate authority (CA) for successful communication and before attempting a checkpassword command to verify connectivity. See the Device certificates and public key infrastructure section of this document.

Example output if ldap-StartTLS is set to required and LDAP certificates are correctly configured:

```
cli% checkpassword test-audit
password:
+ attempting authentication and authorization using system-local data
+ authentication denied: unknown username
+ attempting authentication and authorization using LDAP
+ temporarily setting name-to-address mapping: lr4-gcdc-01.lr4-storage.net -> 16.172.72.91
+ connecting to LDAP server using URI: ldap://lr4-gcdc-01.lr4-storage.net
+ simple bind to LDAP user "test-audit" for DN "LR4-STORAGE\test-audit"
+ searching LDAP using:
        search base:    OU=test,DC=lr4-storage,DC=net
        scope:          sub
        filter:         (&(objectClass=user)(sAMAccountName=test-audit))
        for attributes: memberOf userAccountControl accountExpires lockoutTime
+ search result DN: CN=Test Audit User,OU=test,DC=lr4-storage,DC=net
+ search result:    memberOf: CN=grp-ou-test-audit-global,OU=test,DC=lr4-storage,DC=net
+ search result:    userAccountControl: 66048
+ search result:    accountExpires: 9223372036854775807
+ mapping rule: super mapped to by "CN=grp-test-super-global,OU=test,DC=lr4-storage,DC=net"
+ mapping rule: service mapped to by "CN=grp-test-service-global,OU=test,DC=lr4-
storage,DC=net"
+ mapping rule: edit mapped to by "CN=grp-test-edit-global,OU=test,DC=lr4-storage,DC=net"
+ mapping rule: browse mapped to by "CN=grp-test-browse-global,OU=test,DC=lr4-storage,DC=net"
+ mapping rule: audit mapped to by "CN=grp-test-audit-global,OU=test,DC=lr4-storage,DC=net"
+ rule match: audit mapped to by "CN=grp-test-audit-global,OU=test,DC=lr4-storage,DC=net"
user test-audit is authenticated and authorized
```

Example output if LDAP certificates are not configured and ldap-StartTLS is set to required:

```
cli% checkpassword user_ldap_stig_super
password:
+ attempting authentication and authorization using system-local data
+ authentication denied: unknown username
+ attempting authentication and authorization using LDAP
+ auth param configuration error: Parameter ldap-ssl-cacert is not set
+ authentication denied: configuration error
user user_ldap_stig_super is not authenticated or not authorized
```

OpenLDAP or Red Hat Directory Service

An example configuration to connect to an OpenLDAP server is shown in the following. Many of the connection properties and authentication parameters are shown but exact configuration will vary by environment. For a full reference of all available configuration options, see the HPE Alletra Storage MP B10000 CLI reference guide.

```
cli% setauthparam -f ldap-type OPEN
cli% setauthparam -f ldap-server 10.197.65.32
cli% setauthparam -f ldap-server-hn cxo-st-openldap.lab.hpestorage.com
cli% setauthparam -f binding simple
cli% setauthparam -f groups-dn ou=Groups,dc=systemtest,dc=hpestorage,dc=com
cli% setauthparam -f user-dn-base ou=Users,dc=systemtest,dc=hpestorage,dc=com
cli% setauthparam -f user-attr uid
cli% setauthparam -f group-name-attr cn
cli% setauthparam -f group-obj posixGroup
cli% setauthparam -f member-attr memberUid
cli% setauthparam -f browse-map "cn=ldapguests,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
```

```
cli% setauthparam -f edit-map "cn=ldapoperators,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
cli% setauthparam -f create-map
"cn=ldappowerusers,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
cli% setauthparam -f super-map "cn=ldapadmins,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
cli% setauthparam -f ldap-StartTLS require
cli% importcert ldap -ca stdin
Paste the CA bundle for ldap. Once finished, press Enter twice.
-----BEGIN CERTIFICATE-----
MIIEUTCCAzmgAwIBAgIUbXBQvMBuNQzfeQTMePHFo9YD2o4wDQYJKoZIhvcNAQEL
BQAwgbcxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhDb2xvcmFkbzEMMAoGA1UEBwwD
Q1hPMRswGQYDVQQKDBJIUEUgTmltYmxlIFN0b3JhZ2UxFDASBgNVBAsMC1N5c3Rl
bSBUZXN0MS4wLAYDVQQDDCVjeG8tc3Qtb3BlbmxkYXAubGFiLm5pbWJsZXN0b3Jh
Z2UuY29tMSQwIgYJKoZIhvcNAQkBFhVqZXJlbXkuYmFpbGV5QGhwZS5jb20wHhcN
MjUwMTI0MTgwOTM5WhcNMzUwMTIyMTgwOTM5WjCBtzELMAkGA1UEBhMCVVMxETAP
BgNVBAgMCENvbG9yYWRvMQwwCgYDVQQHDANDWE8xGzAZBgNVBAoMEkhQRSBOaW1i
bGUgU3RvcmFnZTEUMBIGA1UECwwLU3lzdGVtIFRlc3QxLjAsBgNVBAMMJWN4by1z
dC1vc15481dsasdfAdddDSDNMOISH889AmFnZS5jb20xJDAiBgkqhkiG9w0BCQEW
FWplcmVteS5iYWlsZXlAaHBlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMM7yX75t0C8aSeLwinvwkYBVEpOAJ8V8iBuwMX60XDGbg4jSHltq6NI
LAJ48s5ssffXsrx95mDRmmOHzjFO2zVUUp04knXkrkW2J2iEc8TNH4791fegRRAR
skmsSGMg9CluVW74rEPL4jyFmcwGM/weR2ScRyHd6VQit2IpEahixaAb9BXw7mY4
l34RzVK2grzFspq/U/OqWZ126eLAgAwSU9p7FrnUpR532OD/Mw2HTeDKgry3KcnH
Ea9a3/d862LsXQupLewt/tqRTQRpRAKdJ4sL0VxyaaNgERwKxUIO7Ka55ZOmQUJi
JePa2ZHUmb+vJ4wTFJGUH/gqhftOXakCAwEAAaNTMFEwHQYDVR0OBBYEFBuUcJNh
6wZ5vArdWd8uYERym0T/MB8GA1UdIwQYMBaAFBuUcJNh6wZ5vArdWd8uYERym0T/
MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJxGtUKdMtf9CRVs
O+cl3tpWAm0vbvK7VSv/yESh5Ja0B28HVR2io58l9D3XD2HIkxCZEoGP/47fo3S3
4H6aqYsUVS7JzMbW6fetrxB9EwJ+jklCdLZtPIYWEoSd0blxmr9r1hDFVP6Gt0Am
RWfifxH6bhf8r2cDa7FXmhn1xna+girZ6BJxl9TuBdOhG3MQ1L2j/yDk1ddm3Gxz
mZsE1BMp0gt3K39+SmrssxM6TmnRv2xUlwF1BIlpbQ5aQa4bFIP/Azr1SiP0q25O
aW8C6ondvUtJ3O7J5Qxg1x++OVXJGb2QtOrlwqxYcr1uD9Q63GAAnDmBbBHEPSGs
6L74yuY=
-----END CERTIFICATE-----
Do you want to import these certificate(s) for ldap service?
* stdin certificate authorities?
Continue importing signed certificate(s) (yes/no)? yes
cli% checkpassword test
password:
+ attempting authentication and authorization using system-local data
+ authentication denied: unknown username
+ attempting authentication and authorization using LDAP
+ temporarily setting name-to-address mapping: cxo-st-openldap.lab.hpestorage.com ->
10.157.65.32
+ connecting to LDAP server using URI: ldap://cxo-st-openldap.lab.hpestorage.com
```

```
+ simple bind to LDAP user "dg_test" for DN
"cn=test,ou=Users,dc=systemtest,dc=hpestorage,dc=com"
+ searching LDAP using:
        search base:    ou=Users,dc=systemtest,dc=hpestorage,dc=com
        scope:          sub
        filter:         (&(objectClass=posixAccount)(uid=test))
        for attributes: gidNumber
+ search result DN: cn=test,ou=Users,dc=systemtest,dc=hpestorage,dc=com
+ search result:    gidNumber: 2003
+ searching LDAP using:
        search base:    ou=Groups,dc=systemtest,dc=hpestorage,dc=com
        scope:          sub
        filter:         (&(objectClass=posixGroup)(|(gidNumber=2003)(memberUid=test)))
        for attributes: cn
+ search result DN: cn=ldapoperators,ou=Groups,dc=systemtest,dc=hpestorage,dc=com
+ search result:    cn: ldapoperators
+ search result DN: cn=dg_test,ou=Groups,dc=systemtest,dc=hpestorage,dc=com
+ search result:    cn: dg_test
+ mapping rule: super mapped to by
"cn=ldapadmins,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
+ mapping rule: edit mapped to by
"cn=ldapoperators,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
+ mapping rule: browse mapped to by
"cn=ldapguests,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
+ mapping rule: create mapped to by
"cn=ldappowerusers,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
+ rule match: audit mapped to by
"cn=ldappowerusers,ou=Groups,dc=systemtest,dc=hpestorage,dc=com"
user test is authenticated and authorized
```

If ldap-StartTLS is set to **required**, it is also necessary to configure the LDAP client and server certificates before attempting a checkpassword command to verify connectivity. See the Device certificates and public key infrastructure section of this document.

Example output if LDAP certificates are not configured:

```
cli% checkpassword test
password:
+ attempting authentication and authorization using system-local data
+ authentication denied: unknown username
+ attempting authentication and authorization using LDAP
+ auth param configuration error: Parameter ldap-ssl-cacert is not set
+ authentication denied: configuration error
user test is not authenticated or not authorized
```

Multifactor authentication

HPE Alletra Storage MP B10000 supports multifactor authentication with a Department of Defense (DoD) Common Access Card (CAC). CAC login supports two-factor authentication (2FA) of users with the CLI remote client.

CACs are smart identification cards that the DoD issues to individuals. The cards are used to control access to buildings, networks, and systems. A CAC meets the conditions for two-factor authentication (2FA). Something that the user physically has (the card), along with something the user knows (the PIN). An electronic chip, in the card, contains information about the owner, the PIN, and digital certificates.

The CAC login requirements for the storage system include the following:

- **Service account:** Two-factor authentication requires a proxy user called the service account to authenticate and authorize LDAP users. The service account LDAP user name is the full bind DN. Required permission includes read permission for the user and group subtrees. Both ldap-service-account and ldap-service-account-password setauthparam parameters must be set to configure the service account.
- **ldap-2FA-cert-field:** The ldap-2FA-cert-field setauthparam parameter points to where the user's ID lives in their certificate. It can either be in the Subject or Subject Alternative Name field and is configured as follows:
  - Subject uses the prefix **subject**:
  - Subject alternative name uses the prefix **subjectAlt**:. For example: `setauthparam ldap-2FA-cert-field subjectAlt:rfc822name`
- **Object attribute:** The ldap-2FA-object-attr setauthparam parameter points us to where the users' ID lives in their LDAP object. For example: setauthparam ldap-2FA-object-attr mail
- **Trusted CA:** The root CA and intermediate root CA certificates for CACs must be imported to the storage system. The storage system administrators with the super role can import a certificate with the CLI command.

Example

```
cli% setauthparam ldap-service-account <service account name>
cli% setauthparam ldap-service-account-password <service account password>
cli% setauthparam ldap-2FA-cert-field <name of certificate field containing user identity string>
cli% setauthparam ldap-2FA-object-attr <attribute in ldap object corresponding to cert field value>
cli% importcert cac -ca stdin <paste CAC root certificate PEM data>
cli% importcert cac -ca stdin <paste CAC intermediate certificate PEM data>
```

Login banner

Login banners, also referred to as security or notice and consent banners, advise authorized and legitimate users of an organization's acceptable use policy and that activity on the system will be monitored. They can also serve as a definitive warning to possible intruders that certain activity types are illegal, which may be required if prosecution is sought after unauthorized and/or illegal use.

```
cli% showbanner -all
CLI banner:

SSH banner:

cli% setbanner -all
Please enter the text you want to display in the banner below.
Once finished, please press Enter twice.
Note: The maximum number of characters allowed for the text is 4095.

Enter the banner text:
This system is the property of Hewlett Packard Enterprise. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, the Acceptable Use of Information Technology Resources Policy (AUP)
Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized internal and law enforcement personnel, as well as authorized individuals of other organizations. By using
```

```
this system, the user consents to such interception, monitoring, recording, copying,
auditing, inspection, and disclosure at the discretion of authorized personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action,
civil charges/criminal penalties, and/or other sanctions as set forth in the AUP. By
continuing to use this system you indicate your awareness of and consent to these terms and
conditions of use.

cli% showbanner -all
CLI banner:
This system is the property of Hewlett Packard Enterprise. It is for authorized use only. By
using this system, all users acknowledge notice of, and agree to comply with, the Acceptable
Use of Information Technology Resources Policy (AUP)
Any or all uses of this system and all files on this system may be intercepted, monitored,
recorded, copied, audited, inspected, and disclosed to authorized internal and law
enforcement personnel, as well as authorized individuals of other organizations. By using
this system, the user consents to such interception, monitoring, recording, copying,
auditing, inspection, and disclosure at the discretion of authorized personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action,
civil charges/criminal penalties, and/or other sanctions as set forth in the AUP. By
continuing to use this system you indicate your awareness of and consent to these terms and
conditions of use.

SSH banner:
This system is the property of Hewlett Packard Enterprise. It is for authorized use only. By
using this system, all users acknowledge notice of, and agree to comply with, the Acceptable
Use of Information Technology Resources Policy (AUP)
Any or all uses of this system and all files on this system may be intercepted, monitored,
recorded, copied, audited, inspected, and disclosed to authorized internal and law
enforcement personnel, as well as authorized individuals of other organizations. By using
this system, the user consents to such interception, monitoring, recording, copying,
auditing, inspection, and disclosure at the discretion of authorized personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action,
civil charges/criminal penalties, and/or other sanctions as set forth in the AUP. By
continuing to use this system you indicate your awareness of and consent to these terms and
conditions of use.
```

Session management

It is best practice to set session time-outs to the minimal value possible to reduce the time in which a malicious actor can try to steal and use an existing user session.

CLI session time-out

This specifies the value that can be set for an idle CLI session before it times out and closes the connection. Time-out can be set between 180 seconds (3 minutes) and 86399 seconds (23:59:59 hours). Time may be specified in hours, minutes, or seconds providing h or m after the time value and just the value alone for seconds. By default, this is set to 60 minutes.

```
cli% showsys -param
System parameters from configured settings

----------Parameter-----------      ---Value---
RawSpaceAlertSSD               :              0
RawSpaceAlertQLC               :              0
RemoteSyslog                   :              0
RemoteSyslogHost               :        0.0.0.0
RemoteSyslogProfile            :           None
RemoteSyslogSecurityHost       :        0.0.0.0
SparingAlgorithm               :        Default
```

```
EventLogSize                    :             4M
EventLogNum                     :             10
VVRetentionTimeMax              :      336 Hours
UpgradeNote                     :
AutoExportAfterReboot           :            yes
ThermalShutdown                 :            yes
SessionTimeout                  :       01:00:00
OverprovRatioLimit              :            0.0
OverprovRatioWarning            :            0.0
DisableChunkletInitUNMAP        :             no
RemoteCopyHostThrottling        :             no
AutoAdmitTune                   :            yes
SingleLunHost                   :             no
AllowDomainUsersAffectNoDomain  :             no
UpdateAvailability              :            all
EnableAIQoS                     :             no
FastChunkletLogging             :            yes
NVMeoFCEnabled                  :            yes
RelocationDelay                 :    240 Minutes
RwareRetentionTime              :       48 Hours
RwareConfidence                 :         medium
DSCCReadOnly                    :             no

cli% setsys SessionTimeout 10m

cli% showsys -param
System parameters from configured settings

----------Parameter-----------      ---Value---
RawSpaceAlertSSD                :              0
RawSpaceAlertQLC                :              0
RemoteSyslog                    :              0
RemoteSyslogHost                :        0.0.0.0
RemoteSyslogProfile             :           None
RemoteSyslogSecurityHost        :        0.0.0.0
SparingAlgorithm                :        Default
EventLogSize                    :             4M
EventLogNum                     :             10
VVRetentionTimeMax              :      336 Hours
UpgradeNote                     :
AutoExportAfterReboot           :            yes
ThermalShutdown                 :            yes
SessionTimeout                  :       00:10:00
OverprovRatioLimit              :            0.0
OverprovRatioWarning            :            0.0
DisableChunkletInitUNMAP        :             no
RemoteCopyHostThrottling        :             no
AutoAdmitTune                   :            yes
SingleLunHost                   :             no
AllowDomainUsersAffectNoDomain  :             no
UpdateAvailability              :            all
EnableAIQoS                     :             no
FastChunkletLogging             :            yes
```

```
NVMeoFCEnabled                :           yes
RelocationDelay               :   240 Minutes
RwareRetentionTime            :      48 Hours
RwareConfidence               :        medium
DSCCReadOnly                  :            no
```

WSAPI / web server session management

The HPE Alletra Storage MP B10000 WSAPI server session time-out and number of simultaneous logins can be configured.

Session time-out

The session time-out can be set between 3 and 1440 minutes. Changing the session time-out value takes effect immediately and affects already opened and subsequent WSAPI sessions.

```
cli% showwsapi -d
------------------------------WSAPI Server Configuration-------------------------------
service State                          :                                       Enabled
HPE Alletra Storage MP B10000 UI  State  :                                        Active
server State                           :                                        Active
HTTPS Port                             :                                           443
Number of Sessions Created             :                                             0
System Resource Usage                  :                                            96
Number of Sessions Active              :                                             0
Version                                :                                        1.14.0
Event Stream State                     :                                       Enabled
Max Number of SSE Sessions Allowed     :                                             5
Number of SSE Sessions Created         :                                             0
Number of SSE Sessions Active          :                                             0
Session Timeout                        :                                    15 Minutes
Policy                                 :                                no_per_user_limit
API URL                                :   https://s4410.mip.storage.hpecorp.net/api/v1

cli% setwsapi -timeout 10
WSAPI Server configuration set successfully.
```

Simultaneous logins

The limits on the number of simultaneous logins to the WSAPI server are based on user roles.

- In each role type, no user account can have more than 80% of the login sessions.
- For the super and service role types, the default maximum is 11 login sessions (total for the two types).
- For any user account that has the super role, the maximum number of simultaneous login sessions is 9 (11 x 80%).
- For other role types, the default maximum is 51 login sessions per role type.
- The limits are for the total login sessions from all sources, not just the UI.

Login session limits can be configured as follows:

`setwsapi -pol <policy> per_user_limit`. The maximum number of sessions allowed per user is 80% of the system resource usage.

`setwsapi -pol <policy> no_per_user_limit.` The maximum number of sessions allowed per user is the system resource usage.

```
cli% setwsapi -pol per_user_limit
WARNING: The HPE Alletra Storage MP B10000 UI and Web Services API server are enabled and
will restart.
```

```
Are you sure you want to continue?
select q=quit y=yes n=no: y

cli% showwsapi -d
------------------------------WSAPI Server Configuration-------------------------------
service State                          :                                       Enabled
HPE Alletra Storage MP B10000 UI State :                                        Active
server State                           :                                        Active
HTTPS Port                             :                                           443
Number of Sessions Created             :                                             0
System Resource Usage                  :                                            96
Number of Sessions Active              :                                             0
Version                                :                                         1.14.0
Event Stream State                     :                                       Enabled
Max Number of SSE Sessions Allowed     :                                             5
Number of SSE Sessions Created         :                                             0
Number of SSE Sessions Active          :                                             0
Session Timeout                        :                                    10 Minutes
Policy                                 :                                  per_user_limit
API URL                                :   https://s4410.mip.storage.hpecorp.net/api/v1
```

Removing unused accounts

It is prudent to regularly review the local accounts on the system and ensure that only those that are essential are configured. All other nonessential accounts should be removed.

```
cli% showuser
Username        Domain Role    Default
Alletrasnmpuser all    browse  N
adminsvc        all    super   N
stig            all    super   N
stig2           all    super   N
telemetry       all    service N
-------------------------------------
5               total

cli% removeuser stig2
Removing user stig2
select q=quit y=yes n=no: y
User removed
```

Secure network communication

HPE Alletra Storage MP B10000 OS v10.4.0 and later has removed support for TLS 1.1 and earlier; all communication using TLS requires TLS 1.2 or TLS 1.3. 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 2 for U.S. public sector organizations.

With the exception of the VASA service, which can be configured in a TLS 1.3-only mode, all other services utilizing TLS operate in a TLS 1.2 or TLS 1.3 mode.

VASA

The TLS version for the VASA service can be checked and configured as follows:

```
cli% showvasa -config
Key          Value
TLSMethod    tlsv1_2
CopyPriority high
Loglevel     2
Tracing      off
TLSciphers   HIGH:!EXP:!aNULL:!eNULL:!MD5:!RC4:!SSLv3:!TLSv1:!DES:!3DES:@STRENGTH

cli% setvasa -tlsmethod tlsv1_3

cli% showvasa -config
Key          Value
TLSMethod    tlsv1_3
CopyPriority high
Loglevel     2
Tracing      off
TLSciphers   HIGH:!EXP:!aNULL:!eNULL:!MD5:!RC4:!SSLv3:!TLSv1:!DES:!3DES:@STRENGTH
```

Cipher suites in use by VASA can be specified using the setvasa -ciphers command, followed by a list of the ciphers to include or exclude. Lists of cipher suites can be combined in a single cipher string using the **+** character. This is used as a logical AND operation. Each cipher string can be optionally preceded by the characters **!**, **-**, or **+**.

If **!** is used, then the ciphers are permanently deleted from the list. The ciphers deleted can never reappear in the list even if they are explicitly stated.

If **-** is used, then the ciphers are deleted from the list, but some, or all, of the ciphers can be added again by later options.

If **+** is used, then the ciphers are moved to the end of the list. This option does not add any new ciphers and just moves matching existing ones.

Additionally, the cipher string **@STRENGTH** can be used at any point to sort the current cipher list in order of encryption algorithm key length. Note that characters, such as **!**, are significant in most shells and must be escaped or quoted if CLI command is running from another shell.

By default, VASA is configured to only utilize high strength cipher suites and delete export ciphers (EXP), ciphers which do not authenticate (aNULL), do not encrypt (eNULL), MD5, RC4, DES and 3DES which are all deprecated, and other cipher suites associated with SSLv3 and TLSv1.

SNMPv3

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 SNMPv3, 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 SNMPv1 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 SNMPv3.

```
cli% showsnmpuser
no SNMP user listed

cli% createuser Alletrasnmpuser all browse
Password for user Alletrasnmpuser:
Retype password for user Alletrasnmpuser:
User created

cli% createsnmpuser Alletrasnmpuser
Please enter the password to generate authentication key for use in SNMPv3:
Password for user authentication key:
Retype password for user authentication key:
Please enter the password to generate privacy key for use in SNMPv3:
Password for user privacy key:
Retype password for user privacy key:
SNMP user successfully set.

cli% showsnmpmgr
No SNMP managers registered
s2475 cli% addsnmpmgr -version 3 -snmpuser Alletrasnmpuser <SNMPv3 trap recipient IP>
s2475 cli% showsnmpmgr
HostIP        Port SNMPVersion User            Notify   AlertClear
16.172.70.200  162           3 Alletrasnmpuser standard standard

cli% checksnmp
Trap sent to the following managers:
  16.172.70.200:162
```

Device certificates and public key infrastructure

Just as an official government passport establishes a trusted link between a photograph and a person's identity, a signed digital certificate performs a similar function by establishing a link between a network entity and a public key used for cryptography. When this certificate is signed by a trusted CA, it can ensure that the entity you are communicating with on the network is who they say they are.

X.509 v3 is the current standard defining the format of public key certificates and was developed by the International Telecommunication Union. A selection of the data that can be contained in a X.509 certificate is listed in Table 1. For the complete format, see RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Table 1. Data contained in X.509 certificates

Certificate data	Description
Version number	X.509 certificate version—v3 is the most recent
Serial number	Unique serial number of the certificate assigned by the certificate authority
Signature algorithm ID	Cryptographic algorithm used for the digital signature (for example, SHA-256 with RSA encryption)
Issuer name	Entity that issued the certificate
Validity period	The date the certificate is valid from, and the date it expires
Subject	Details of the network entity the certificate belongs to. For example, common name, organization, locality, country
Subject public key information	The algorithm used, key length and public key of the certificate
Extensions (v3 certificates only)	Multiple extensions can be specified including, but not limited to, subject alternative names, key usage, extended key usage, CRL distribution lists

Although self-signed certificates are sometimes convenient, they do not provide any degree of trust during communication, and if compromised, can be a gateway for malicious actors to gain access to the network. In addition, they can also inadvertently train users to be less security-conscious when visiting other websites. When users grow accustomed to bypassing the untrusted certificate warning on a website for an internal application such as HPE iLO or GUI, it does not take long for a habit to form and for users to click through warnings on malicious or compromised websites.

It is always advisable to use X.509 certificates signed by a trusted certificate authority for any array service.

Client certificates

Multiple device services require CA signed X.509 certificates for secure communication between client and server. The client certificates are the array's identity certificates, which will be presented to the server in a TLS handshake. Table 2 lists the array services that use X.509 certificates for communication purposes.

Table 2. HPE Alletra Storage MP B10000 client certificate services

Service	Details	CLI service name
Unified server	Provides a common device certificate for CIM, CLI, and WSAPI services—these can also be configured separately	unified-server
LDAP	For secure LDAP authentication	ldap
Secure syslog	For security syslog communication	syslog-sec-client
External key manager (EKM)	For external key manager communication	ekm-client
VASA	For VASA communication	vasa
Quorum witness	For Quorum witness communication	qw-client

Installing a CA-signed certificate follows three steps:

- Generating a certificate signing request
- Having the certificate authority generates a signed certificate from the CSR
- Installing the CA-signed certificate along with the CA certificate authority chain

```
cli% showcert -service <service name>
cli% createcert <service name> -csr -CN <common name> [optional subject attribute options] -
SAN DNS:<fqdn>,IP:<IP address>
```

Table 3. HPE Alletra Storage MP B10000 CLI certificate signing request options

Options	Description
-CN <common name>	Specifies the value of the common name (CN) attribute of the certificate subject.
-O <organization>	Specifies the value of the organization (O) attribute of the certificate subject.
-OU <organizational unit>	Specifies the value of the organizational unit (OU) attribute of the certificate subject.
-L <locality>	Specifies the value of the locality (L) attribute of the certificate subject.
-ST <state>	Specifies the value of the state (ST) attribute of the certificate subject.
-C <country>	Specifies the value of the country (C) attribute of the certificate subject.
-SAN <subject_alt_name[,subject_alt_name]...>	Subject alternative name is an X.509 extension that allows other pieces of information to be associated with the certificate. Multiple SANs may be delimited with a comma.

To include CSR attributes that contain spaces, write the attributes inside double quotation marks (for example, -O "Hewlett Packard Enterprise").

Copy the CSR output and submit it to the certificate authority for signing.

```
cli% importcert <service name> [-f] stdin stdin
```

Copy and paste the signed certificate PEM data and the CA bundle PEM data as instructed.

Example

```
cli% showcert -service ekm-client

There are no certificates for the following service(s): ekm-client

cli% createcert ekm-client -csr -CN test-user -SAN DNS:s2475.lr4-storage.net

-----BEGIN CERTIFICATE REQUEST-----
MIICjDCCAXQCAQAwFDESMBAGA1UEAwwJdGVzdC11c2VyMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxKv9qxzITdZOu6d4vm8TXeH1H1gE8Pi4bAbtQ7yp
KTIQd/E9jinoeRmFYA6ulU8YB8HRsfQ/4Ld7v9/Kwatu6OUEnA2DG618Z+wWYfuR
BI00RiqJwb82E6O00Q0oacnR+4/nqtiWmQkABFFtXIE7hJFJXgLRyat9+n3uJJYr
F0wIJFa46DoUBG1ZEaoKVFD7ubkC1US2NRyIeLz/oG0TI9yYZcRo8OWvkuYexGF6
13azqV0eP8avs7r2LvIk32YV+JShwdRPsIbTJTnPPo1oar+AY0l2vyBMx169jY9y
jWZynu1gMNTdcBmYuLDUfssV9tJtXtZRMddGqDw/swxRJwIDAQABoDMwMQYJKoZI
hvcNAQkOMSQwIjAgBgNVHREEGTAXghVzMjQ3NS5scjQtc3RvcmFnZS5uZXQwDQYJ
KoZIhvcNAQELBQADggEBABCcwPJaMpkKv9CrYqyidPJmx1D5o0Ldvc+VTNoI9aaK
HG29sf2DOfjhA+qbP9mkBs4w29HTcMikgPkC34+RHX7E4UfnXNifE7vfTbMfEZfK
l1VUjnagbMTfwQ4SQb+deqP++tLJ5aj2BDb+R1cRbht3p98GGSjVHc1BwgJO/N5a
Vv+l3EAvb6g7BX8Q4oUUnGCF6a4ZGJQfeh+wctYx+2GKPK5EA6EX+xWq39U95lpU
CMkJX0FiBzK6Ck2ZcDeC6jc2inrNQMB9Un0f0f4DQRDjxhyPw03B6TQmJGZ/DLiZ
m8UmjofbkyNVsmGnCcdjZgCDIvCIFRoqQPxZC9iTydw=
-----END CERTIFICATE REQUEST-----
```

```
cli% importcert ekm-client -f stdin stdin

Please paste the Certificate for ekm-client. Once finished, please press Enter twice.
-----BEGIN CERTIFICATE-----
MIIE0jCCArqgAwIBAgIQI7F4htN4jys046eBpjL5ozANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEPMA0G
A1UEChMGVGhhbGVzMRwwGgYDVQQDExNDaXBoZXJUcnVzdCBSb290IENBMB4XDTI0
MDYwNzIwNDAxMloXDTM0MDMxMTEwMjQ0MlowFDESMBAGA1UEAxMJdGVzdC11c2Vy
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxKv9qxzITdZOu6d4vm8T
XeH1H1gE8Pi4bAbtQ7ypKTIQd/E9jinoeRmFYA6ulU8YB8HRsfQ/4Ld7v9/Kwatu
6OUEnA2DG618Z+wWYfuRBI00RiqJwb82E6O00Q0oacnR+4/nqtiWmQkABFFtXIE7
hJFJXgLRyat9+n3uJJYrF0wIJFa46DoUBG1ZEaoKVFD7ubkC1US2NRyIeLz/oG0T
I9yYZcRo8OWvkuYexGF613azqV0eP8avs7r2LvIk32YV+JShwdRPsIbTJTnPPo1o
ar+AY0l2vyBMx169jY9yjWZynu1gMNTdcBmYuLDUfssV9tJtXtZRMddGqDw/swxR
JwIDAQABo4HZMIHWMA4GA1UdDwEB/wQEAwIDiDATBgNVHSUEDDAKBggrBgEFBQcD
AjAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFN9hqtCSI/QShiKSypRMZZUbCHB3
MCAGA1UdEQQZMBeCFXMyNDc1LmxyNC1zdG9yYWdlLm5ldDBeBgNVHR8EVzBVMFOg
UaBPhk1odHRwOi8vY2lwaGVydHJ1c3RtYW5hZ2VyLmxvY2FsL2NybHMvMzMzM2Qw
YmQtNWYzZS00Yjg5LThhMzYtZmY2NzhiYjllYzU4LmNybDANBgkqhkiG9w0BAQsF
AAOCAgEARPqaKoqluXH5B3hbyNqKTj4kHVQeNKLmKYMn7kLhd6byORT9LgNScBlF
2A2Tc1NFS5fOgYXzGOjEDd2kByYn40IEsnSlS+jBkKbr+p4pEz7xbpoD7FS8VpMG
UmBhXUYIPPez10U60x68ZoaZfeDorCounhifMVJ7PIH19MD9ssgrC7ptYb+2UmAp
3Er8epKnS2Np+k0dKglOSK2TZr7SGO3pFMIMPPiJgGhTr4jSngg/WULEh1x08ik+
L8V99ZirggukmE+733eeRiobX89AWgg/vvGvRYyMRPcQ4fah2MrKins9Ffn+7yuE
FODOin/QDR3ivc1+WpjMVKFlC+qBStGUEREijCsKjNFtAJoJygUjnUfFlNTbN1CR
HozZeatXfSBA3Iwh79bSMCzRqOJpMQXomn15VTYWB9G0HBLaXYW4znEPS6TgtLRK
cw2vbq2ETTebuomlOfdG92QPQM4XVppFKBVHKYmWKW+RBSidcTCpxIkg4pA7mw76
b85RNWNLRbc8pGM5Ws02EG5V1yoPRfXsa8VLmVVNRPlVQ13PBju8knTyOavXTz61
NCgLImCTZ8lGQr4S8UdUhiqE6HcE60k6C9+UDFx2WJ0CFUIipXW7arLnXmy2xGbF
fCA/rNf0qKhyG3oY6+XsIgP52rUhGH4JVbvoSMxr8CE0wdTNK7o=
-----END CERTIFICATE-----
Please paste the CA bundle for ekm-client. Once finished, please press Enter twice.
-----BEGIN CERTIFICATE-----
MIIFrjCCA5agAwIBAgIQKsgy+vDEnzzGJ00XuAlIfDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEPMA0G
A1UEChMGVGhhbGVzMRwwGgYDVQQDExNDaXBoZXJUcnVzdCBSb290IENBMB4XDTI0
MDMxMjEwMjQ0MloXDTM0MDMxMTEwMjQ0MlowWjELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAlRYMQ8wDQYDVQQHEwZBdXN0aW4xDzANBgNVBAoTBlRoYWxlczEcMBoGA1UE
AxMTQ2lwaGVyVHJ1c3QgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBAO3v2C6kMG7DCb0S2v2EJdtOMWwDrCims+SB33qM1cvgZGmdkSmMFHPL
bVYkS4yVNi5WQvhf8wgplo0VJfqVhUE+0/iCGCMaQQsWGc7D0XxR9Y2Us5CxryBs
BGvVWXCM7Cmw846jtLqMvOb3N3wO6rW+IxGQz3aKvOxf/CHUA56FfjI2BEqbK7n4
SidNPB4jL5WWRBHtoeeKWJlhHEY4ipOjiirorP4pvW+zk5TdFENsv/fLKYMyoH3E
```

```
Z1P0NZ22vXvv/0o5+669p4KSVGV5VeUHRQeptUtvhQU1CT+XbrIhBxHeaTf0rYR0
T6NvmtCeQ/WyyCftPSivQWl45TadYfLzaB2G3biaVqo76WWxONKDxwPxj+caaJ9Z
xJK2TffYEl1+9qnSBVvGiMOlfO9g3TPCWjlRsu/4t1L8YvBbG6yivDQVcBInV5eS
izRbHSAs8JTiFezohXdA0exbOunEK+wJ4aDzJ54X6EuiUM7ZTR+xU/kGzIKaKK96
y3bBGWc6US60CDhkobl+tJMwbVd+AzwX7aikbNdA+VJoGmxydlxnISouwcB6nJAK
ip+PYmedL5LYJKaqe24BB0Ar5ob37X/V331qd087QSIcCOuZdNVvybvxM9Gvg19P
PYw+SH/kEUxikpVbDDTgls9D0S7qXAaIPWfz5v0UYMlz2bP+7qsfAgMBAAGjcDBu
MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTfYarQ
kiP0EoYiksqUTGWVGwhwdzAsBgNVHREEJTAjgSF0ZWNobmljYWwuc3VwcG9ydEB0
aGFsZXNncm91cC5jb20wDQYJKoZIhvcNAQELBQADggIBALiItF3ONQElKO1l+3oX
gKP5QLtBceO4prYoKdNQW+eSHcx8Sq398/u8AcUvvBlGMhUMUfsROsCAFpI1hO1I
WnemjNx7/GbrvjrVdMHee6mMTk3PJat5lBwj/4aSzqV/cRvSLUaVuiqsgZEGQMDN
mSc0CXi+Fq9fEIGC+bDajcPKT3S655X7oJ5nzqM311Ao7cvGernZujnNrqHFTfof
kGcgH3NBXh/DOQZx+yznmOSbICn9QSPJNe58vvUInaECdYKMi0SSpOTP5bbBJ4iN
5GeRPDJu9ou94+83TgV2oPOIBMgdTfNlCN9ONrvg+RKLmilb5ajixA63sLSYNPn/
LUxhv41srwhkN0bb5HGD7nqpjkGRxMz73i/qIG7eH5fzCQX3NUD2kwXn0YB7CREu
VL+9bACSXlDkPatrPDXqAnPnlrncVI8FDpbmkriP4pCLtpPUu71SwUWK+LqwHGJV
y03ia4out/m/sU9IjmYiFo1mZsw7uaNh9kA24jAIOEg+FVr0lgA7anBmPydM7bqO
hMfA+OM6SEam7TERP1t/soOkmSSniFJ1gx7HEq2+tgeDP3tnkL0qN9MPfp2d37cJ
t7XF3n/YgbZEOp//Floyn9JIuWTP0M7MMnHegA7Gy29imYsx2v5eg2ll3JEUs779
aCJ2UTznCtIqbiGKlDlwQcbT
-----END CERTIFICATE-----

cli% showcert -service ekm-client
Service     Commonname          Type    Enddate                  Fingerprint
ekm-client  test-user           cert    Mar 11 10:24:42 2034 GMT
f05f859bb2f141af8666ce9b9601c2b7b01d2ed0
ekm-client* CipherTrust Root CA rootca Mar 11 10:24:42 2034 GMT
c2b3e77b89279d830299d60561152b2bedbf6ef6
```

Server certificates

Server certificates are required when the HPE Alletra Storage MP B10000 system is acting as a client to an external server, such as an external key manager. For communication to be trusted, the root CA certificate from the server's certificate authority chain must be imported. Often, but not always, this can be the same root CA certificate that signed the client certificate; however, it still must be imported and registered against the server SSL service.

Table 4. HPE Alletra Storage MP B10000 server certificate services

Service	Details	CLI service name
Secure syslog	Root CA for the security syslog server	syslog-sec-server
Syslog	Root CA for the general syslog server	syslog-gen-server
External key manager	Root CA for the external key manager	ekm-server
Quorum witness	Root CA for the Quorum witness server	qw-server
Common account card	Root CA for the CAC for two-factor authentication	cac

The same process is used as importing signed client SSL certificates, specifying the service and using the -ca flag to specify it as a root CA certificate.

```
cli% importcert <service name> [-f] -ca stdin
```

Example

```
cli% importcert ekm-server -ca stdin

Please paste the CA bundle for ldap. Once finished, please press Enter twice.
-----BEGIN CERTIFICATE-----
MIIFmDCCA4CgAwIBAgIQEz6/R4aRzr1CJGW2OIlczTANBgkqhkiG9w0BAQsFADBL
MRMwEQYKCZImiZPyLGQBGRYDbmV0MRswGQYKCZImiZPyLGQBGRYLbHI0LXN0b3Jh
Z2UxFzAVBgNVBAMTDmxyNC1zdG9yYWdlLUNBMB4XDTIyMDUzMTE3Mjg1MFoXDTMy
MDUzMTE3Mzg0NFowSzETMBEGCgmSJomT8ixkARkWA25ldDEbMBkGCgmSJomT8ixk
ARkWC2xyNC1zdG9yYWdlMRcwFQYDVQQDEw5scjQtc3RvcmFnZS1DQTCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAL4rFacYmmrmLrjlkkCUYBonZ8AGf/Xu
KXAPufa7ta+B4wk+wPmKckT3vaIUeG6yf8Q5KmvQq3cPfnsZZghobkl/CUpPXKI1
BoBXHXocrsdxNROnr/hN1hTcDCZRcz8ww8SrnkoFLFkK48qHKM9NkKsDvIOZyElG
yMGOyLeCOOQ5vyyQBc2b/FmHyyJFUjrKryO133G3xFTOtsCf85kTizSpwrh1l7zc
0/114iATNlRO5ZlU987rmWrOaOApCMGplUoZU3lXBVTh4gfZNURXWJUjBN8SwHHo
fNJeTmxY0IcKLEWZIZS6wwdtKvcTmoD35qMta5D76fKGM+YgEIvCzUT4pRC3tfJo
68ludbt+1D0Dd/C08fCgB9dbvJ9ZNJlJhfyeGjUe3cIEDkmvz9KsGDAl4CwUWAJj
YR98HCi1swQjSGYNluojQIXGHJOhqAx1HLwmFfYww1LVBKlzkdcCVQMLV4T1D0Ne
idVcMqD7k6BuCOGMFUBElM6Mz5mOOUJ9OafLL1bXiGeN50SaHfqJRuXONJOAsH4c
QWgZKJpdECZARuEtCR4zNzP8SMYRPmw7npxwfbqYIUvdL5jIA+q9FSEq54Wmpc6u
7BCBboypsUAcANzgbBA5Ug4nnTGhzSY+BlZ99xjcPqjaKQAX8FKfakYKqJwOHVVG
+l4rFouquOXNAgMBAAGjeDB2MAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/
MB0GA1UdDgQWBBTQtBdI2LXVMl937xb6Z/EJWnooYDASBgkrBgEEAYI3FQEEBQID
AgACMCMGCSsGAQQBgjcVAgQWBBTchvdBv5wf8bWU25jo8Qs+vVzsATANBgkqhkiG
9w0BAQsFAAOCAgEAnVuwGyWj+pXXaSkbHhgyt5Z28jlEojobizcRF3IbrBjODOSY
mPcOrlDWZeor66vxYw1yEG4EFMdKLG6e3lNqioG8KFuGHXQphaB1gMe5PYrVCqVs
h8kyBp7YZfI2NT2678RzbtGGHOiLeGNJz79eIiXMQNjWEq8kgN6E0hBCen74rRcs
OHd5ciL9h74p0y/nCj6hE31StGnFHS7TSNta1jFbBx70IsL3Ci8ovW7lIY+4KSoE
U88/1ZCrbDZif4XKl9qJLy1SM21k1rpafmodPVOkwaE8SmGCQf0MRHtnpoiao/Vv
R5vF3pdvj1X1AT2mD1AMI2EyvqF9N9X2hx1LZp9rYqsFjV984k+BnfGpiBaL97pA
lsqZrJv23uxg7P+QKkBHQgTnmY8uHyL011gBK5K3XjX6LqB7b9MxknGMU9ntg5UF
7dgYMc4i8jf99J3tJCEjZwo/6njLAxIuHBlaoslMOWfCyr8JvZ/9YyF3LIR9HXhs
N4mE9gwwpNj0+Pl+vEiaxkO/et2iLRv7Na6pXBFxYhvtcNrXqt8uAgrMMHklS7Ub
grGFYVMuUcqMOjTSCrJKXk9r7qkuRJCxSdMd45XY8TK14hQ7luokS1ejR5WCSiG/
qxbvezU1yLDlSmFiHWxnLW6oNUGW3tBOUdykrFRMTm/tfmcKtHiODXfO8ag=
-----END CERTIFICATE-----

Do you want to import these certificate(s) for ekm-server service?
* stdin certificate authorities?
Continue importing signed certificate(s) (yes/no)? yes

cli% showcert -service ldap

Service Commonname     Type   Enddate                  Fingerprint
ekm-server    lr4-storage-CA rootca May 31 17:38:44 2032 GMT
409e507985813f294f9c9464e488e46d903f4f58
```

Usually only the root CA certificate is required; however, there are some instances where intermediate CA certificates may need to be installed alongside the root certificate. Run the same command again after installing the root CA certificate but using the PEM data from the intermediate CA certificate. The root CA certificate must always be installed first.

Compliance and reporting

Cybersecurity compliance is the requirement for an organization to adhere to laws, standards, and regulatory requirements that may be applicable to their business and geography. HPE Alletra Storage MP B10000 provides several functions to help achieve compliance and ensure accurate reporting of system activities.

FIPS mode

FIPS mode is a setting that enforces 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.

To check the current FIPS mode status:

```
cli% controlsecurity fips status
FIPS mode: Disabled

Service      Status
AUTHN        Disabled
CIM          Disabled
CLI          Disabled
EKM          Enabled
LDAP         Disabled
QW           Disabled
RDA          Disabled
SC CONNECTOR Disabled
SNMP         Disabled
SSH          Disabled
SYSLOG       Enabled
VASA         Disabled
WSAPI        Enabled
----------------------
13           3 Enabled
```

To enable FIPS mode:

```
cli% controlsecurity fips enable
```

After enabling FIPS mode, it is advisable to check the status again to ensure all services show enabled:

```
cli% controlsecurity fips status
FIPS mode: Enabled

Service      Status
AUTHN        Enabled
CIM          Enabled
```

```
CLI          Enabled
EKM          Enabled
LDAP         Enabled
QW           Enabled
RDA          Enabled
SC CONNECTOR Enabled
SNMP         Enabled
SSH          Enabled
SYSLOG       Enabled
VASA         Enabled
WSAPI        Enabled
----------------------
13           13 Enabled
```

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 HPE Alletra Storage MP B10000 Security Guide to ensure compatibility, so communication is not disrupted when enabling CC mode.

The status of CC mode can be checked with the command:

```
cli% controlsecurity cc status

CC mode is disabled
```

To enable CC mode:

```
cli% controlsecurity cc enable

Warning: Enabling CC mode requires restarting all SSH Sessions,
which will terminate ALL existing connections including this one.
When that happens, you must reconnect to continue.
Continue enabling CC mode (yes/no)? yes

Connection to 192.168.12.10 closed by remote host.
Connection to 192.168.12.10 closed.


cli% controlsecurity cc status

CC mode is enabled
```

To disable CC mode:

```
cli% controlsecurity cc disable

Warning: Disabling CC mode requires restarting all SSH Sessions,
which will terminate ALL existing connections including this one.
When that happens, you must reconnect to continue.
Continue disabling CC mode (yes/no)? yes
Connection to 192.168.12.10 closed by remote host.
Connection to 192.168.12.10 closed.

cli% controlsecurity cc status
CC mode is disabled
```

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 security syslog server, to which messages associated with user login actions and changes to the encryption management settings are sent. The security syslog server can be a valuable early warning system providing real-time alerts of potentially malicious access attempts to the array.

The syslog configuration and status can be checked with the command:

```
cli% showsys -d
```

Example output when no syslog server is configured

```
-----Remote_Syslog_Status------
Active              :         0
General Server      :   0.0.0.0
General Connection  :      None
RemoteSyslogProfile :      None
Security Server     :   0.0.0.0
Security Connection :      None
```

Example output when syslog servers are configured

```
----------Remote_Syslog_Status-----------
Active              :                   1
General Server      :      16.10.3.94:514
General Connection  :                 UDP
RemoteSyslogProfile :         majorEvents
Security Server     :     16.10.3.94:6514
Security Connection :                 TLS
```

General syslog

```
cli% setsys RemoteSyslogHost {{<hostname>|<IPv4>}[:<port>]|<IPv6>|[<IPv6>]:<port>},..
```

Up to three syslog servers can be specified, separated with commas. If no port is specified, one of the following default ports will be used: UDP/514, TCP/601, TLS/6514. For syslog connections over TLS, the syslog-gen-server CA certificate must be installed to establish secure communication. See the Device certificates and public key infrastructure section of this document for more information.

Profiles can be applied to the general syslog server to filter which syslog messages are sent to the server. By default, all message categories are sent.

```
cli% setsys RemoteSyslogProfile {<profile>|None}
cli% showsys -syslogprofile
Profile_Name      Description
allAlerts         Pass through all Alerts and Service Alerts
majorEvents       Pass through operational events with Major, Critical and Fatal severity
operationalEvents Pass through all operational events
userObjectChange  Pass through events logging configuration changes to system objects
```

Security syslog

```
cli% setsys RemoteSyslogSecurityHost {{<hostname>|<IPv4>}[:<port>]|<IPv6>|[<IPv6>]:<port>},..
```

Up to three security syslog servers can be specified, separating with commas. Security syslog messages must be sent over TLS; if no port is specified, the default port of 6514 will be applied. Security syslog messages over TLS require syslog-sec-client and syslog-sec-server certificates to be installed to establish secure communication. See the Device certificates and public key infrastructure section of this document for more information.

Event log capacity

The size of the event log and the number of retained event logs in addition to the active file can be configured.

```
cli% EventLogSize <value>
```

Sets the size of the event log—the range is between 0.5 MiB and 10 MiB with the default being 5 MiB.

```
cli% setsys EventLogNum <value>
```

Can be configured between 1 and 30, with the default being 10.

Verify that the event log is successfully generating messages with the showeventlog [options <arg>] command.

Example

```
cli% showeventlog -nsev information -nsev minor -nsev degraded -more
```

This command will show all event log entries excluding informational, minor, and degraded severities being displayed one page at a time.

Example output

```
Time       : 2025-01-24 21:15:36 PST
Severity   : Major
Type       : Cage SSH authorized keys updated
Message    : Cage cage41 (0x51402EC018DE62FE) I/O Module 2 SSH authorized keys updated with
the latest node keys.
Time       : 2025-01-24 21:15:36 PST
Severity   : Major
Type       : Cage SSH authorized keys updated
Message    : Cage cage42 (0x51402EC018DE64AA) I/O Module 1 SSH authorized keys updated with
the latest node keys.
```

Network Time Protocol

Inaccurate time stamps make it more difficult to correlate events and can lead to inaccurate analysis in the event of an incident. By synchronizing internal information system clocks, uniformity of time stamps across systems connected over a network can be achieved.

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 preshared cryptographic keys. This preshared 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.

Configuring NTP

NTP servers can be configured using the setnet command:

```
cli% shownet
IP Address   Netmask/PrefixLen Nodes Active Speed Duplex AutoNeg Status Mode
16.182.44.22     255.255.224.0  0123      3  1000 Full   Yes     Active Static
Default IPv4 route :                              16.182.32.1
Default IPv6 route :                                     None
NTP server         :                                     None
DNS server         :   16.182.80.91 16.182.80.92 16.182.80.93
Proxy server       :                  http://10.78.90.46:8080
cli% setnet ntp -add <server ip address>
cli% shownet
IP Address   Netmask/PrefixLen Nodes Active Speed Duplex AutoNeg Status Mode
16.182.44.22     255.255.224.0  0123      3  1000 Full   Yes     Active Static
Default IPv4 route :                              16.182.32.1
Default IPv6 route :                                     None
NTP server         :                           ntp.hpecorp.net
DNS server         :   16.182.80.91 16.182.80.92 16.182.80.93
Proxy server       :                  http://10.78.90.46:8080
```

A maximum for four NTP servers can be configured.

Configuring NTP with authentication

NTP authentication allows an NTP client to verify the authenticity of an NTP server using preshared cryptographic keys. This preshared 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.

The NTP keys must be added to the NTP configuration on both the client and the server. For NTP, the HPE Alletra Storage MP B10000 array acts as an NTP client.

To import the keys a key file must be imported into the array using the format:

keyno type key

The following message digests and ciphers are supported by the HPE Alletra Storage MP B10000: SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, TIGER, WHIRLPOOL, AES128, AES256, AEAD-AES-SIV-CMAC-256. MD5 and SHA1 message digests are not supported.

Example

11 AES256 HEX:C9D94B5563DBEB2F2E855DF2ACAE2817EB185070CFE7CCB7CDCBF49632967BAC

```
cli% importkeys ntp ntp.keys
NTP server successfully updated.
cli% showkeys ntp
ID Type   Value
11 AES256 C9D94B5563DBEB2F2E855DF2ACAE2817EB185070CFE7CCB7CDCBF49632967BAC
```

To configure the NTP server with authentication on the storage array, the -key option must be used:

```
cli% setnet ntp -add -key 11 -prefer 16.182.3.94
NTP configuration successfully updated.
```

Configuring the time zone

Configuring the system time zone allows log entries to be mapped to the universal time code (UTC) to allow for accurate correlation of system events.

```
cli% showdate

Node Date
0    2025-02-04 07:20:50 PST (America/Los_Angeles)
1    2025-02-04 07:20:49 PST (America/Los_Angeles)
2    2025-02-04 07:20:49 PST (America/Los_Angeles)
3    2025-02-04 07:20:49 PST (America/Los_Angeles)

cli% setdate -tzlist

Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Brazil
Canada
Chile
Etc
Europe
Indian
Mexico
Pacific
US


cli% setdate -tzlist <time zone group>

Example
cli% setdate -tzlist US
US/Alaska
US/Aleutian
US/Arizona
US/Central
US/East-Indiana
US/Eastern
US/Hawaii
US/Indiana-Starke
US/Michigan
US/Mountain
US/Pacific
US/Samoa

cli% setdate -tz <time zone group/location>
```

```
Example

cli% setdate -tz US/Pacific
```

Data-at-rest encryption

DAR encryption requires a combination of compatible **self-encrypting drives (SEDs)** and a valid encryption license. It can be enabled nondisruptively at any time—even after data has been written to the system. There is no need for existing data to be rewritten, and there is no impact on drive performance because data written to SEDs is always encrypted by the onboard encryption module. Enabling DAR encryption on HPE Storage arrays changes the **authentication key (AK)** that is used to access the drives and enables drive lock if power to the drive is lost. It does not enable encryption on the drive itself because that is always enabled. After DAR encryption is enabled on the array, it **cannot** be disabled. Data-at-rest encryption in this instance refers to the data being encrypted as it is written to the SED by its onboard cryptoprocessor and its corresponding decryption, as it is read from the SED.

External key managers

To comply with FIPS 140-2 standards, the authentication key (AK) used to access the self-encrypting drives must be stored in a FIPS 140-2 certified external key manager. Rather than having the AK and associated metadata stored on the array in the persistent repository (PR) and in the backup file, the key is generated by and stored on the EKM. In this case, the PR and backup file contain configuration metadata, including a copy of the required TLS certificates needed to establish EKM connectivity. Communication between the array and the EKM is conducted through a secure TLS channel using the **Key Management Interoperability Protocol (KMIP)**. This protocol enables you to store the keys for multiple arrays in a centralized, clustered, secure location. Individual backup files must still be recorded and maintained by the security officer for each array so that EKM connectivity can be recovered in a disaster recovery scenario.

Multiple EKM servers can be configured as a cluster for redundancy (up to a maximum of four); these must all be of the same type. In this case, the key is stored on each element in the cluster. For example, the key is created on EKM node 1, which takes care of the replication to the other nodes, but each EKM server in the cluster must be specified when configuring the EKM on the array.

Before configuring the EKM server settings, the ekm-server and ekm-client certificates must be present on the array. See the Device certificates and public key infrastructure section of this document, or for a more detailed look at data-at-rest encryption on HPE Alletra Storage MP B10000 MP arrays, see the HPE Alletra Storage MP B10000 data-at-rest encryption technical white paper.

To configure the EKM:

```
cli% controlencryption setekm -setserver ekm1.example.com,ekm2.example.com -port 5696

-ekmuser username -kmipprotocols 1.0,1.1,1.2,1.3,1.4

Password for EKM user:

cli%


cli% controlencryption setekm -addserver ekm3.example.com

cli% controlencryption setekm -removeserver ekm3.example.com
```

Note

`The port, ekmuser, ekmpass, and kmipprotocols` options apply to all EKM servers configured.

Use either of the following command to display the current encryption status and a list of configured EKM servers:

```
cli% showencryption -d
```

Example output

```
Licensed Enabled BackupSaved State  SeqNum Keystore FIPS   non-SEDs FailedDisks nodeNonSED

yes      yes     yes         normal      1 EKM      Compliant           0           0
0


Number of EKM servers defined: 2
EKM servers: ekm1.example.com, ekm2.example.com

EKM server port: 5696

EKM username: a9k
KMIP Protocols: 1.0,1.1,1.2,1.3,1.4
```

To verify if the settings are correct and the array can successfully communicate with the external key manager, run the following command:

```
cli% controlencryption checkekm
EKM settings are correct
```

Enabling data-at-rest encryption

Once DAR encryption is enabled, it cannot be disabled. The first time DAR is enabled on a system if no key manager flag is specified, the system will use the local key manager (LKM); an external key manager can be specified with the -ekm flag. The controlencryption -enable command is also used if transitioning between key managers, for example, from an external key manager to a local key manager. In this instance, the -lkm flag can be used to specify using the LKM.

```
cli% controlencryption -enable <-ekm>
```

Note

See the HPE Alletra Storage MP B10000 data-at-rest encryption technical white paper for a detailed description of the process of migrating between key managers.

Reducing the attack surface

The attack surface of a system is the area that may be susceptible to unauthorized access. The smaller the attack surface, the easier it is to protect a system. Therefore, it is advisable to disable any functionality that is not required for the proper operation of a system and to close any ports that are not in use or deemed insecure.

Disabling nonencrypted ports

Where possible, communication using TCP should be encrypted using TLS to ensure the confidentiality of data being transmitted across the network. Disabling nonencrypted ports blocks certain, additional, ports that the standard firewall does not, except internal loopback and internode interfaces. Additionally, it blocks unencrypted communications for additional services on the management interface, for example, VASA, WSAPI and CIM.

Nonencrypted ports can be disabled using the following command:

```
cli% setnet disableports yes

Disabling non-encrypted ports will disable Recovery Manager for VMware® and SRA.
Disabling non-encrypted ports should only be done if there is a strict
requirement for all connections to be encrypted.

Are you sure you want to disable non-encrypted ports?
select q=quit y=yes n=no: y
```

Disabling unused functions

It is always wise to disable functionality outside of the scope of requirements, as any unused features can increase risk by providing additional attack vectors.

Remote copy

If the **remote copy** feature is not required, it can be disabled.

```
cli% showrcopy -d

Remote Copy System Information
Status: Started, Normal

cli% stoprcopy

cli% showrcopy -d

Remote Copy System Information
Status: Stopped, Normal
```

Data Services Cloud Console read-only mode

Data Services Cloud Console (DSCC) is a secure cloud application, deployed on the 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.

DSCC communicates with the HPE Alletra Storage MP B10000 via REST API, using an internal user account for authentication. This can be set to allow only read-only access allowing DSCC users to view the array settings but not modify them.

DSCC read-only mode status can be viewed with the command:

```
Cli% showsys -param
System parasmeters from configured settings

----------Parameter-----------      --------------------Value--------------------
RawSpaceAlertSSD               :                                              0
RawSpaceAlertQLC               :                                              0
RemoteSyslog                   :                                              0
RemoteSyslogHost               :                                        0.0.0.0
RemoteSyslogProfile            :                                           None
RemoteSyslogSecurityHost       :       192.168.12.102:6514,192.168.12.104.65140
SparingAlgorithm               :                                        Default
EventLogSize                   :                                             4M
EventLogNum                    :                                             10
VVRetentionTimeMax             :                                      336 Hours
UpgradeNote                    :
AutoExportAfterReboot          :                                            yes
ThermalShutdown                :                                            yes
SessionTimeout                 :                                       00:10:00
OverprovRatioLimit             :                                            0.0
OverprovRatioWarning           :                                            0.0
DisableChunkletInitUNMAP       :                                             no
RemoteCopyHostThrottling       :                                             no
AutoAdmitTune                  :                                            yes
SingleLunHost                  :                                             no
AllowDomainUsersAffectNoDomain :                                             no
UpdateAvailability             :                                            all
EnableAIQoS                    :                                             no
FastChunkletLogging            :                                            yes
NVMeoFCEnabled                 :                                            yes
RelocationDelay                :                                    240 Minutes
RwareRetentionTime             :                                       48 Hours
RwareConfidence                :                                         medium
DSCCReadOnly                   :                                             no

DSCC read-only mode is enabled with the command:

cli% setsys DSCCReadOnly yes
cli% showsys -param

System parameters from configured settings

----------Parameter-----------      --------------------Value--------------------
RawSpaceAlertSSD               :                                              0
```

```
RawSpaceAlertQLC               :                                              0
RemoteSyslog                   :                                              0
RemoteSyslogHost               :                                        0.0.0.0
RemoteSyslogProfile            :                                           None
RemoteSyslogSecurityHost       :       192.168.12.102:6514,192.168.12.104.65140
SparingAlgorithm               :                                        Default
EventLogSize                   :                                             4M
EventLogNum                    :                                             10
VVRetentionTimeMax             :                                    336 Hours
UpgradeNote                    :
AutoExportAfterReboot          :                                            yes
ThermalShutdown                :                                            yes
SessionTimeout                 :                                       00:10:00
OverprovRatioLimit             :                                            0.0
OverprovRatioWarning           :                                            0.0
DisableChunkletInitUNMAP       :                                             no
RemoteCopyHostThrottling       :                                             no
AutoAdmitTune                  :                                            yes
SingleLunHost                  :                                             no
AllowDomainUsersAffectNoDomain :                                             no
UpdateAvailability             :                                            all
EnableAIQoS                    :                                             no
FastChunkletLogging            :                                            yes
NVMeoFCEnabled                 :                                            yes
RelocationDelay                :                                    240 Minutes
RwareRetentionTime             :                                     48 Hours
RwareConfidence                :                                       medium
DSCCReadOnly                   :                                            yes
```

DSCC read-only mode can be disabled with the command

```
cli% setsys DSCCReadOnly no
```

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 resources covered in this document enable administrators to harden the configuration of an HPE Alletra Storage MP B10000 array in-line with the U.S. Department of Defense (DoD) Security Requirements Guide (SRG), considering both the current threat environment and capabilities of the product.

Resources

HPE Alletra Storage MP B10000 architecture

Data Services Cloud Console Security Guide

HPE Alletra Storage MP B10000 MP data-at-rest encryption technical white paper

HPE Alletra Storage MP B10000: CLI reference

HPE Alletra Storage MP B10000 security guide

HPE Alletra Storage MP B10000: cyber resilience with data-adaptive ransomware detection

Learn more at

HPE.com/us/en/Alletra-Storage-MP-B10000.html

Visit HPE.com

Chat now

a00146015ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com