Cohesity Solution Guide for Sheltered Harbor

NetBackup 11.2

VERITAS
now part of Cohesity

Sheltered Harbor Solution Guide

Last updated: 2026-05-28

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

About Cohesity Sheltered Harbor solutions

This chapter includes the following topics:

About Sheltered Harbor

Sheltered Harbor protects public confidence in the U.S. financial system if a devastating event like a cyberattack causes an institution's critical systems - including backups - to fail.

The Sheltered Harbor solution is for U.S. financial institutions of all types and sizes and is your lifeline to survival in an extreme cyber, data corruption or data deletion event. It ensures you to remain connected with your customers and can continue to serve them with essential services, within hours of a catastrophic event that has caused all your critical systems - including backups - to fail. Sheltered Harbor Specifications provide that "fail-safe", thereby enhancing your institutions' resilience, reputation, and customers' trust .

The following are the three core elements of the Sheltered Harbor solution:

- Data Vaulting

- Resilience Planning
- Certification

Data Vaulting

Institutions back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault is encrypted, unchangeable, and completely separated from the institution's infrastructure.

Resilience Planning

Institutions prepare the business and technical processes and key decision arrangements to be activated in the case of a Sheltered Harbor event; where all other options to restore critical systems - including backups - have failed. Sheltered Harbor resilience plan enables the participating financial institution to quickly recover the critical account data from the vault and restore two critical services: customer access to account balance information, and access to funds against those balances.

Certification

Participating institutions adopt a robust set of Sheltered Harbor prescribed safeguards and controls, which are independently audited for compliance with the Sheltered Harbor standards. Upon successfully completing the requirements for Data Vaulting, the institution will be awarded Sheltered Harbor Data Protected certification and an accompanying seal, communicating that their customer account data is protected. Additional certification is awarded to organizations that demonstrate completed and tested resilience plans.

About Sheltered Harbor solutions

Sheltered Harbor's endorsement of NetBackup confirms that it meets Sheltered Harbor's prescribed Data Vaulting Solution Requirements and provides a secure environment for the daily data vaulting process:

- Immutable storage: During a cyberattack, the vault remains immutable and the data cannot be erased or modified in any worst-case scenario.
- Survivable vault: The vault is accessible even when the institution's infrastructure fails. The financial institution can retrieve the data easily and maintain continuous access to essential processes.
- Controlled environment: The decentralized environment secures the data from being tampered. Data is easily accessible and is kept separate from the institution's infrastructure.

To enable and use the Sheltered Harbor functionality within the NetBackup Sheltered Harbor Solution (including certification), institutions must first sign-up to participate in Sheltered Harbor.

https://shelteredharbor.org/join

Consequently, institutions that implement the NetBackup client properly should be able to achieve certification more quickly and easily.

Data vaulting in Sheltered Harbor solutions

Sheltered Harbor solution backs up the financial institution's critical customer account data every day in the Sheltered Harbor standard format. The Sheltered Harbor solution is implemented in NetBackup client where daily vaulting process is run to make the backup readily available.

The backup data is encrypted, unchangeable, and completely separated from the institution's infrastructure. The Sheltered Harbor solution runs the daily vaulting process that supports the following options that can back up the data:

- Cohesity Alta™ solution for Sheltered Harbor
  See "About Cohesity Alta solution for Sheltered Harbor" on page 8.
- Cohesity NetBackup™ solution for Sheltered Harbor
  See "About NetBackup for Sheltered Harbor" on page 12.

About Cohesity Alta solution for Sheltered Harbor

The Cohesity Alta solution for Sheltered Harbor implements Sheltered Harbor standards to run daily data vaulting process and to persist data in an immutable cloud-based vault.

Cohesity recommends the Cohesity Alta Recovery Vault multi-cloud immutable storage service with air-gapped isolation that protects data from cyber threats that is a predictable as-a-service subscription offering. The cloud-based storage-as-a-service provides a seamless, fully managed storage option to store critical data. The institution data remains secure in the cloud and protected from the ransomware.

For more information, refer to the Cohesity Alta Recovery Vault documentation.

Cohesity Alta Recovery Vault supports the following:

- Archive data vaulting using Cohesity Alta Recovery Vault for Sheltered Harbor
  See "Archive data vaulting using Cohesity Alta Recovery Vault for Sheltered Harbor" on page 9.

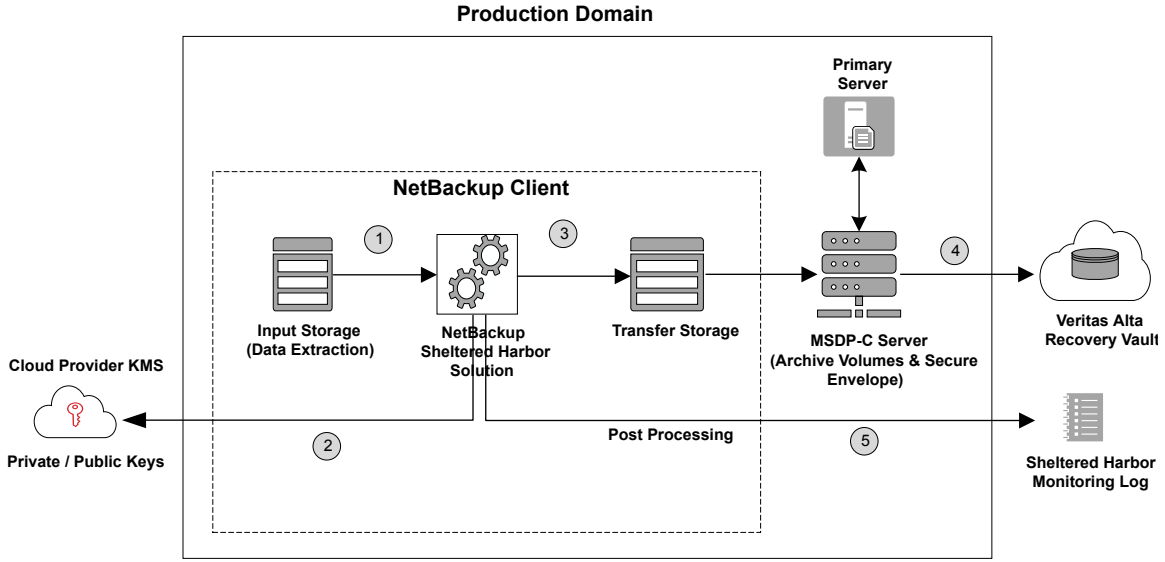
- Archive restoration using Cohesity Alta Recovery Vault for Sheltered Harbor
  See "Archive restoration using Cohesity Alta Recovery Vault for Sheltered Harbor" on page 10.

Archive data vaulting using Cohesity Alta Recovery Vault for Sheltered Harbor

In this process, the selected data is stored on the cloud using immutable storage and the original files are available on the source. To start the data vaulting operation, the backup policy needs to be configured on the NetBackup primary server. When you start the data vaulting operation, the NetBackup client software on your computer sends the data to be backed up to the NetBackup media server. The media server then deduplicates and writes the data to a supported immutable cloud object storage. After the data backup is successful, the Sheltered Harbor solution sends an attestation message to Sheltered Harbor monitoring log.

The Sheltered Harbor solution on the NetBackup client initiates the backup of encrypted data. The following diagram depicts the process of data backup to Cohesity Alta Recovery Vault:

Figure 1-1 Archive data vaulting using Cohesity Alta Recovery Vault for Sheltered Harbor



The process flow is as follows:

1. Input storage: The input storage includes manifest, account data files, and corresponding hash files that originated from the institution. At this stage, the input data is extracted using the Sheltered Harbor solution and is processed further for input data validation. Here, it generates an archive volume and encrypts it using the data encryption key. It also generates the secure envelope that stores the cryptographic material of encryption.
2. External or cloud provider KMS: The NetBackup Sheltered Harbor solution encrypts the input storage data using data encryption key (DEK) and this DEK is further encrypted with the help of a configured external KMS or cloud-provider based KMS. It ensures that the encryption or decryption keys do not leave the KMS boundaries. If cloud KMS is not configured, you can use on-premises KMS.
3. Transfer storage: The input data files are compressed and encrypted to generate encrypted archive volumes and are stored in the transfer storage.
4. Immutable cloud storage: NetBackup deduplicates and stores the encrypted volume and secure envelope to a supported immutable cloud object storage such as Cohesity Alta Recovery Vault during the backup process. A unique keyword is generated and is used during backup. This keyword identifies the backup image during restore and it can be seen using `--report` command option. For example, 'SH-<random number>' keyword is generated during backup that is further used on the BAR UI to see the backup files.

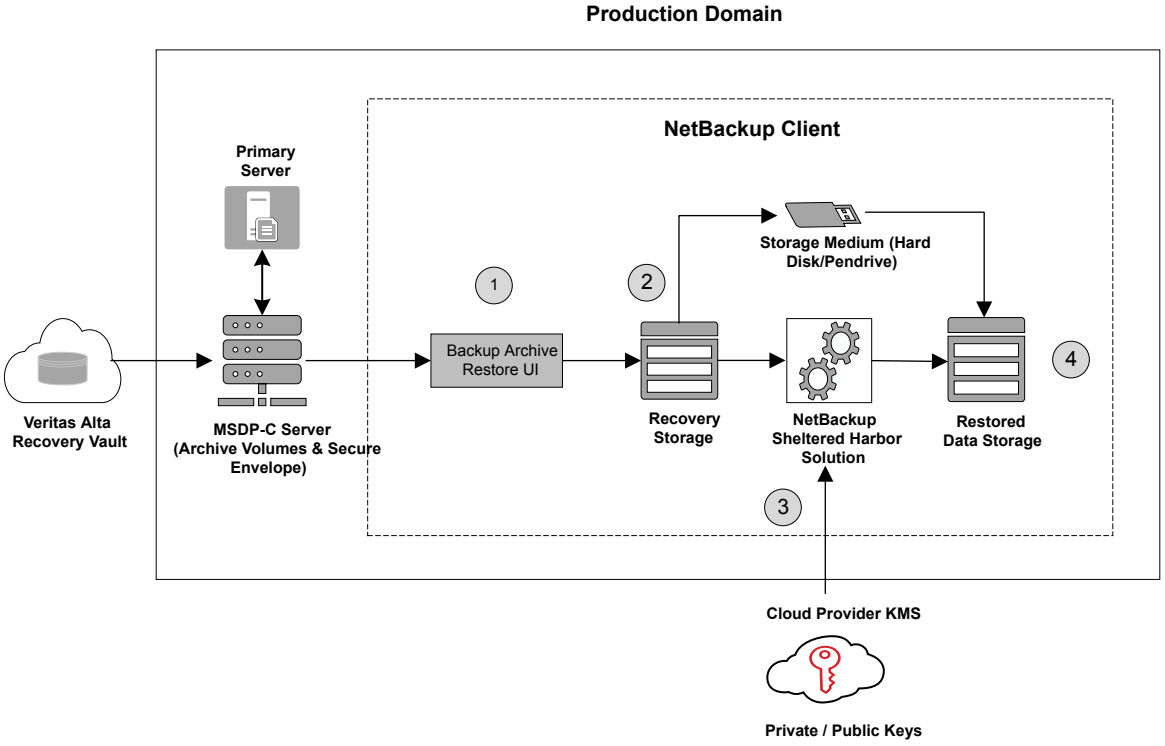
   Note: The Sheltered Harbor solution supports either CohesityAlta Recovery Vault or an Isolated Recovery Environment (IRE) to be configured for the data vaulting operations. Other NetBackup storage unit types are not supported.

5. Sheltered Harbor monitoring log: The Sheltered Harbor monitoring log shows the attestation message as a proof of a successful completion of the daily data vaulting process.

Archive restoration using Cohesity Alta Recovery Vault for Sheltered Harbor

Data restoration is carried out to restore the data if required using the restore command option. The Sheltered Harbor solution on the NetBackup client decrypts and restores the data. The following diagram depicts the process to restore the data from Cohesity Alta Recovery Vault.

Figure 1-2 Archive restoration using Cohesity Alta Recovery Vault for Sheltered Harbor



The process flow is as follows:

1. Archive retrieval: From the NetBackup client, you need to manually restore the backup data using NetBackup Backup Archive Restore (BAR) UI or NetBackup web UI. You need to use the backup keyword to restore the data.

   See "Restore backup data using NetBackup web UI" on page 19.

2. Data restoration: The recovery storage contains the retrieved encrypted data files along with the secure envelope. You can use any portable medium (such as pen drive, hard disk) to store the restored data. The portable media can be transferred to the third-party restoration platform to restore data and services.

Note: Ensure that you specify the correct recovery storage path while you restore the backup data files using the BAR GUI or web UI.

---

3 External or cloud provider KMS: The NetBackup Sheltered Harbor solution decrypts the data encryption key (DEK) with the help of a configured external KMS or a cloud-provider based KMS. The DEK is further used to decrypt the recovery storage data. It ensures that the encryption or decryption keys do not leave the KMS boundaries. If cloud KMS is not configured, you can use on-premises KMS.

Note: The decryption of data by the solution is required only for data recovery and verification test, or for service restoration by a self-restorer.

4 Restored data storage: Once you perform the data restoration using the Sheltered Harbor solution, the data files are decrypted and stored in the restored data storage.

The data restoration using the Sheltered Harbor solution can be done on a completely isolated NetBackup client that does not have a connectivity with a primary server. Such isolated NetBackup client can be installed by skipping host certificate deployment during NetBackup client install. The data restoration needs a connectivity with KMS where envelope decryption key is stored.

Note: Ensure that you specify the correct restoration storage path while performing the data restoration operation.

About NetBackup for Sheltered Harbor

The NetBackup™ for Sheltered Harbor solution implements Sheltered Harbor standards to run daily data vaulting process. Isolated Recovery Environment (IRE) enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files. This is on demand to neutralize the impact from a ransomware attack.

The NetBackup Isolated Recovery Environment solution:

- Ensures data is immutable and indelible – minimizing threats from both ransomware and rogue users.
- Detects ransomware infections within the protected data to prevent reinfection when restoring data.
- Enables recovery operations at scale so business services can meet service level objectives.

- Enables predictable recovery processes that can be rehearsed to on-premises or cloud infrastructure.

NetBackup for Sheltered Harbor supports the following:

- Archive data vaulting to Air-gapped Cyber Resilient Domain (CRD)
- Archive restoration in Cyber Resilient Domain (CRD)
- Archive recovery in Cyber Resilient Domain (CRD) and restoration in restoration environment

Archive data vaulting to Air-gapped Cyber Resilient Domain (CRD)

In this process, the selected data is backed up and replicated to Cyber Resilient Domain (CRD) and leaves the original files on the source. To start the data vaulting operation, the backup policy that uses storage lifecycle policy (SLP) with IRE capable storage unit, needs to be configured on the production NetBackup primary server.

When you start the data vaulting operation, the NetBackup client software on your computer sends the data to be backed up to the NetBackup media server that runs in the production domain. That media server then replicates it to media server that runs in CRD domain and subsequently it is imported in CRD NetBackup primary server. This process ensure that a copy is created on immutable storage that is present in the CRD domain and is completely isolated from the production domain.

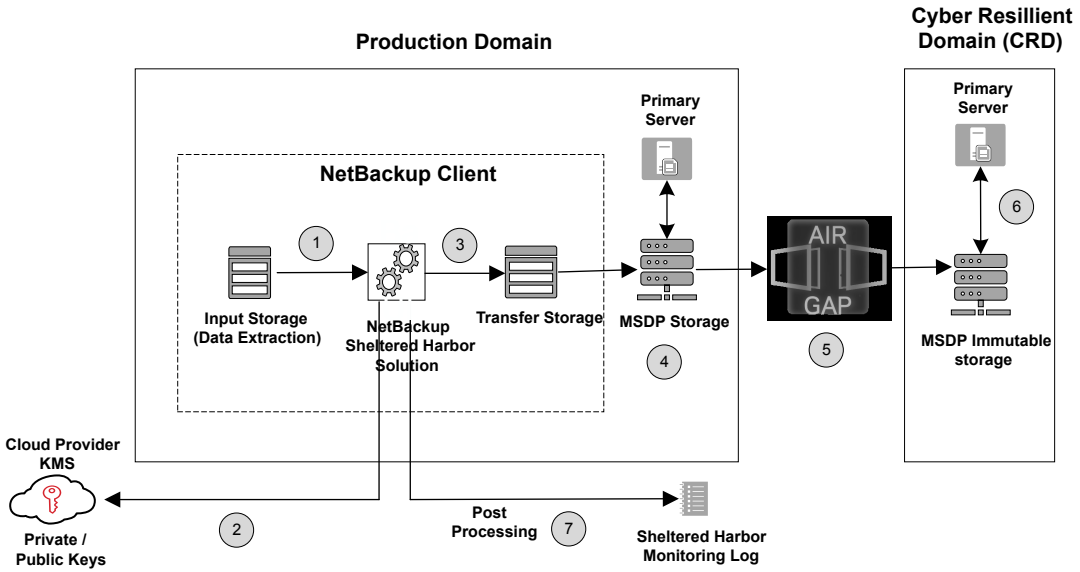
After a copy of the data is created in the immutable storage, the Sheltered Harbor solution sends an attestation message to the Sheltered Harbor monitoring log.

Note: Sheltered Harbor solution requires outbound connections to be open from CRD primary server to production primary server so that import notification works.

Import notification is sent to the production domain that indicates that the copy of SLP images is completed in the CRD domain.

The Sheltered Harbor solution on the NetBackup client initiates the backup of encrypted data. The following diagram depicts the process of data vaulting to CRD domain:

Figure 1-3 Data vaulting using NetBackup for Sheltered Harbor



The process flow is as follows:

1 Input storage: The input storage includes manifest, account data files, and corresponding hash files that originated from the institution. At this stage, the input data is extracted using the Sheltered Harbor solution and is processed further for input data validation.

Here, it generates an archive volume and encrypts it using the data encryption key. It also generates the secure envelope that stores the cryptographic material of encryption.

2 External or cloud provider KMS: The Sheltered Harbor solution encrypts the input storage data using data encryption key (DEK) and this DEK is further encrypted with the help of a configured premises KMS. It ensures that the encryption/decryption keys do not leave the KMS boundaries. If cloud KMS is not configured, you can use on-premises KMS.

3 Transfer storage: The input data files are compressed and encrypted to generate encrypted archive volumes and are stored in the transfer storage.

4. Backup in production domain: The encrypted archive volumes along with secure envelope get backed up on a production MSDP storage unit first. A unique keyword is generated and is used during backup. This keyword identifies the backup image during restore and it can be seen using –-report command option. For example, 'SH-<random number>' keyword is generated during backup that is further used on the BAR UI to see the backup files.

   Note: The Backup operation runs successfully without configuring IRE import notification.

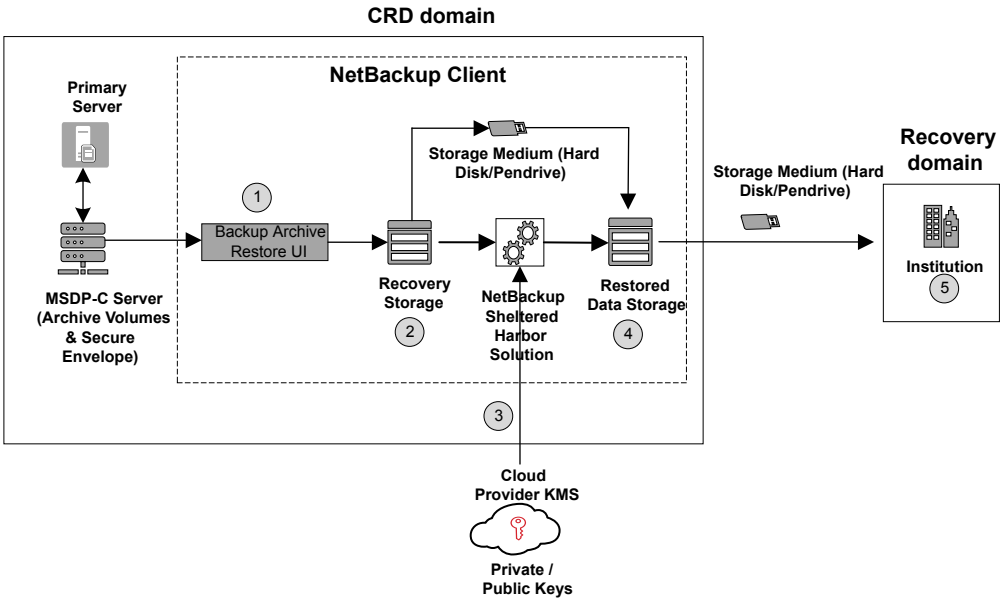
5. Air gap: The air gap restricts network access to data stored on MSDP server running in CRD domain except during time-frame when replication occurs from production MSDP to CRD MSDP server. Once the encrypted archive volumes along with secure envelope get backed up in production domain, NetBackup initiates replication of that backup image only when logical air gap is closed.
6. Import in CRD domain: Once the image is replicated to CRD domain, the import operation imports the image in CRD domain ensuring that a copy of encrypted archive volumes and secure envelope, is made on immutable storage in CRD domain. After successful import, a notification is sent to Production Primary server.
7. Sheltered Harbor monitoring log: The Sheltered Harbor solution keeps polling for import notification from CRD domain. Once it receives that an attestation message as a proof of a successful completion of the daily data vaulting process is sent to Sheltered Harbor monitoring Log.

Archive restoration in Cyber Resilient Domain

Data restoration is carried out to restore the data if required using the restore command option. The Sheltered Harbor solution on the NetBackup client decrypts and restores the data.

The following diagram depicts the process to restore the data using NetBackup for Sheltered Harbor solution in CRD domain.

Figure 1-4 Archive restoration in Cyber Resilient Domain



The process flow is as follows:

1 Archive retrieval: From the NetBackup client, you need to manually restore the backup data using NetBackup Backup Archive Restore UI (BAR GUI) or NetBackup Web UI. While restoring, you need to use the backup keyword to restore the data.

See "Restore backup data using NetBackup web UI" on page 19.

Note: Make sure that the recovery storage path should be empty while restoring the backup data files because the data files cannot be overwritten.

2 Recovery storage: It contains the recovered encrypted data files along with the secure envelope. You can use any portable medium (such as Pen drive, hard disk) to store the recovered data.

Note: Make sure that you specify the correct recovery storage path while restoring the backup data files. Use the NetBackup Backup Archive Restore UI to restore the data.

3. External or cloud provider KMS: The Sheltered Harbor solution decrypts the data encryption key (DEK) with the help of a configured KMS. The DEK is further used to decrypt the recovery storage data. It ensures that the encryption/decryption keys do not leave the KMS boundaries. If cloud KMS is not configured, you can use on-premises KMS.
4. Restored data storage: Once you perform the data restoration using the Sheltered Harbor solution, the data files are decrypted and stored in the restored data storage.

   The data restoration using Sheltered Harbor solution can be done on a completely isolated NetBackup client that does not have a connectivity with a primary server. Such isolated NetBackup client can be installed by skipping host certificate deployment during NetBackup client install. The data restoration needs a connectivity with KMS where envelope decryption key is stored.

   Note: Ensure that you specify the correct restoration storage path while performing the data restoration operation.

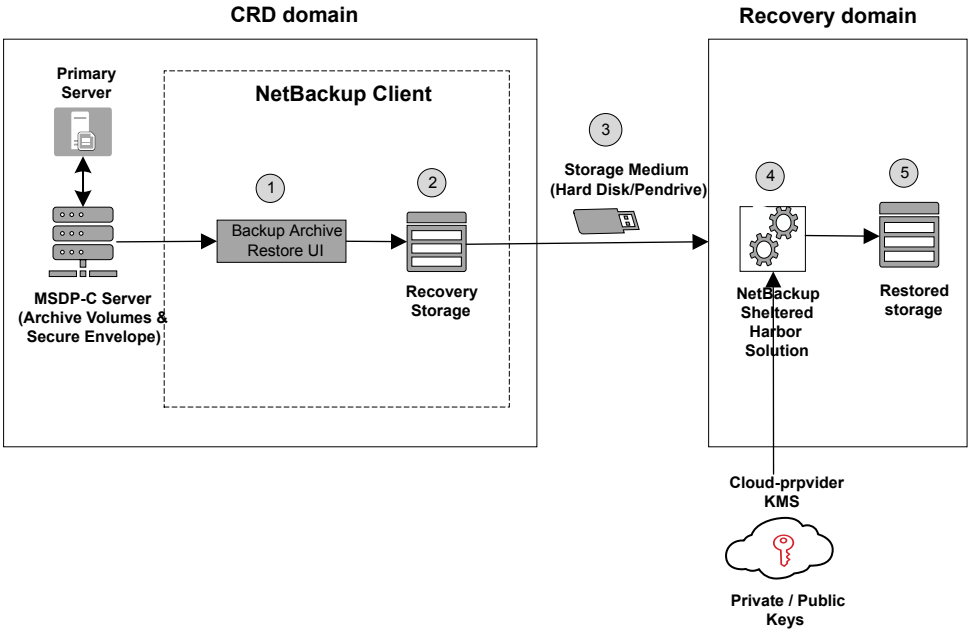
5. Recovery domain: Once the files are stored in the restored data storage, you can transfer the data to recovery domain by using any portable medium (such as Pen drive, hard disk).

Archive recovery in Cyber Resilient Domain (CRD) and restoration in restoration environment

Here the archived volumes are recovered in CRD domain and data restoration is carried out in Recovery domain using the restore command option. The Sheltered Harbor solution on the NetBackup client decrypts and restores the data.

The following diagram depicts the process to recover the data in CRD domain and restore it in Recovery domain using NetBackup for Sheltered Harbor solution.

Figure 1-5 Archive recovery in Cyber Resilient Domain (CRD) and restoration in restoration environment



The process flow is as follows:

1. Archive retrieval: From the NetBackup client, you need to manually restore the backup data using NetBackup Backup Archive Restore UI (BAR GUI) or NetBackup Web UI in the CRD domain. While recovering, you need to use the backup keyword to recover the data.

   See "Restore backup data using NetBackup web UI" on page 19.

2. Recovery storage: It contains the recovered encrypted data files along with the secure envelope. You can use any portable medium (such as Pen drive, hard disk) to store the restored data.

   Note: Make sure that you specify the correct recovery storage path while recovering the backup data files. Use the NetBackup Backup Archive Restore UI to recover the data or NetBackup web UI.

3. Data transfer: Use any portable medium (such as Pen drive, hard disk) to transfer the encrypted data files to the Recovery domain to initiate data decryption by using Sheltered Harbor solution.

4 External or cloud provider KMS : The Sheltered Harbor solution decrypts the data encryption key (DEK) with the help of a configured KMS. The DEK is further used to decrypt the recovery storage data. It ensures that the encryption/decryption keys do not leave the KMS boundaries. If cloud KMS is not configured, you can use on-premises KMS.

5 Restored data storage: Once the recovered data available in Restoration environment, the Sheltered Harbor solution is run to perform the data restoration which decrypts archived volumes and extract data files and store in the restored data storage.

The data restoration using Sheltered Harbor solution can be done on a completely isolated NetBackup client that does not have a connectivity with a primary server. Such isolated NetBackup client can be installed by skipping host certificate deployment during NetBackup client install. The data restoration needs a connectivity with KMS where envelope decryption key is stored.

Note: Ensure that you specify the correct restoration storage path while performing the data restoration operation.

Restore backup data using NetBackup web UI

Use the following procedures to restore the backup data using NetBackup web UI:

To restore the backup data

1 Log into NetBackup web UI. See Sign in to the NetBackup web UI for more information.

2 On the left, click **Recovery**.

3 Under **Regular recovery**, click **Start recovery**.

4 Select the following properties:

- Source client
  The client that performed the backup.
- Destination client
  The client to which you want to restore the backup.
- Policy type

Note: For UNIX, use the standard policy type. For Windows, use the MS-Windows policy type.

- Restore type
  You need to use normal backups type.

5 Click **Next**.

6 Select the **Start date** and **End date**.

7 Select **Backup Keyword** that was used during backup. You can run the `--report` command option to see the keyword.

8 Select the files that needs to be restored using the file explorer.

Note: All the files in the image need to be selected for restore. If they are not selected, the Sheltered Harbor solution does not recover the files.

---

9 Click **Next**.

10 Select **Restore target options** as required. If **Restore everything to a different location** is selected, then provide the directory used as **Recovery storage path** for Sheltered Harbor solution.

11 Click **Next**.

12 Review the recovery settings and then click **Start recovery**.

Chapter 2

Prerequisites to configure Sheltered Harbor solutions

This chapter includes the following topics:

Common prerequisites to configure Sheltered Harbor solutions

Review the given prerequisites that are applicable for both Sheltered Harbor solutions.

NetBackup installation

The NetBackup Sheltered Harbor solution is available on all NetBackup server platforms.

The following are the steps to install NetBackup primary server, media server, and client.

Table 2-1 Installation Overview

Step	Description
Step 1	Install the NetBackup primary server software on your system. See NetBackup Installation Guide.
Step 2	Install the NetBackup media server software on your system. See NetBackup Installation Guide.
Step 3	Install the NetBackup client software on your system. See NetBackup Installation Guide.

System requirements

Review the following system requirements for the NetBackup Sheltered Harbor solution:

- NetBackup primary server: Version 10.2
- NetBackup media server: Version 10.2
- NetBackup client: Version 10.2

Note: NetBackup version 10.2 is highly recommended for NetBackup primary, media server, and client roles. Limited NetBackup deployment types for BYO and Flex Appliance are supported using version 10.1

KMS: Use either of the following KMS services:

- Cloud KMS (CKMS): Azure key vault based external KMS solutions is supported.
- On-premises KMS (EKMS): See External KMS - Considerations in the Encryption and Security Solutions section for more information.

Note: NetBackup KMS cannot be used for the Sheltered Harbor solution configuration.

Note: The solution validates the CRL of the KMS user certificate before performing cryptographic operations. To download the CRL, you should update the `ECA_TRUSTSTORE_PATH` configuration option.

See "ECA_TRUST_STORE_PATH for NetBackup servers and clients" on page 26.

If the NetBackup host is already configured with external CA, you should append the external CA certificate to the existing path.

The service user must have the read permissions on the CA certificate file.

Immutable cloud storage: An immutable cloud storage provider is required to support Sheltered Harbor specific standards. See cloud storage vendor compatibility list with either of these two designations.

- S3 Object Lock: Yes
- Object Lock (Immutable storage): Yes

Operating system: For information on the operating system requirements for the NetBackup primary server, media server and client, see NetBackup Compatibility List.

Prerequisites to configure Alta solution for Sheltered Harbor

To configure Alta Recovery Vault and create a policy, do the following:

Table 2-2 Configuration Overview

Step	Description
Step 1	To configure Alta Recovery Vault (formerly known as NetBackup Recovery Vault), see Alta Recovery Vault Deployment Guide.
Step 2	To create a policy, see the Creating backup policies chapter in NetBackup Administrator's Guide, Volume 1. While creating the policy, you must select the user backup schedule to configure the policy. For the NetBackup Sheltered Harbor solution, the retention period must be greater than 2 days. **Note:** For UNIX, use the standard policy type. For Windows, use the MS-Windows policy type. **Note:** Ensure that the client host name used in backup policy is exactly same as CLIENT_NAME field in client's NetBackup configuration.

Note: You must get the license from the Sheltered Harbor before configuring the NetBackup Sheltered Harbor solution and make sure to renew the license before it expires.

Prerequisites to configure NetBackup solution for Sheltered Harbor

To configure NetBackup for Sheltered Harbor solution, do the following:

Table 2-3 Configuration Overview

Step	Description
Step 1	To configure Auto Image Replication (A.I.R.), see About Auto Image Replication (A.I.R.).
Step 2	To configure Isolated Recovery Environment (IRE), see Configuring isolated recovery environment (IRE).
Step 3	To configure the Isolated recovery Environment (IRE) for Sheltered Harbor solution. See "Configuration of Isolated Recovery Environment (IRE)" on page 24.
Step 4	To create a policy, see the Creating backup policies chapter in NetBackup Administrator's Guide, Volume 1. While creating the policy, you must select the user backup schedule to configure the policy. For the NetBackup Sheltered Harbor solution, the retention period must be greater than 2 days. **Note:** For UNIX, use the standard policy type. For Windows, use the MS-Windows policy type. **Note:** Ensure that the client host name used in backup policy is exactly same as CLIENT_NAME field in client's NetBackup configuration.

Configuration of Isolated Recovery Environment (IRE)

To configure the IRE for Sheltered Harbor solution, do the following:

To configuring IRE

- On UNIX systems, the directory path to the following commands is `/usr/openv/netbackup/bin/admincmd`
- On Windows systems, the directory path to following commands is `install_path\NetBackup\bin\admincmd`

1. Set SLP lifecycle parameter *SLP.ENABLE_IMPORT_CONFIRMATION* = *1* in Production and IRE domain. Use the following command:

   ```
   # bpsetconfig

   bpsetconfig> SLP.ENABLE_IMPORT_CONFIRMATION = 1
   ```

2. Add IRE primary server as Trusted Master in production primary. Use the following command:

   ```
   # bpsetconfig

   bpsetconfig> TRUSTED_MASTER = <IRE primary server name>
   ```

3. Update remote primary server version of IRE primary in production domain. Use the following command:

   ```
   # nbemmcmd -updatehost -machinename <IRE primary server name>
   -machinetype remote_primary -netbackupversion <NetBackup version>
   ```

4. Add production primary server as remote primary server in IRE domain. Use the following command:

   ```
   # nbemmcmd -addhost -machinename <Production primary server name>
   -machinetype remote_primary -netbackupversion <NetBackup version>
   -operatingsystem <OS name>
   ```

   - On UNIX systems, the directory path to the following commands is `usr/openv/netbackup/bin/`
   - On Windows systems, the directory path to the following commands is `install_path\NetBackup\bin\`

5. Deploy HostID certificate for IRE primary server from Production Primary server. Use the following command:

   ```
   # nbcertcmd -getCACertificate -server <production primary server>

   # nbcertcmd -getCertificate -server <production primary server>
   -token <token>
   ```

   Note: If you are using ECA enroll certificate on IRE primary server then, run the following command.

   ```
   # nbcertcmd -enrollCertificate -server <production primary server>
   ```

Configuration of Flex

Cohesity NetBackup solution for Sheltered Harbor is supported on Cohesity Flex Appliance 2.1 and later.

To configure Flex Appliance for Sheltered Harbor solution

1. Configure Flex Appliance.
2. Configure NetBackup primary server, media server, and WORM storage server instance on Flex Appliance.
3. Configure Isolated Recovery Environment (IRE) on Flex Appliance.
4. Configure IRE for Sheltered Harbor solution.

   See "Configuration of Isolated Recovery Environment (IRE)" on page 24.
5. NetBackup client can be installed on a separate host and associated with the NetBackup Flex primary server instance.

   Configure the NetBackup for Sheltered Harbor solution on the same client.

   The NetBackup solution for Sheltered Harbor is also supported on Cohesity Flex Scale Appliance 3.2 and later.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The `ECA_TRUST_STORE_PATH` option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the `ECA_TRUST_STORE_PATH` option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

The root CA certificate in Cloudera distribution can be obtained from the Cloudera administrator. It may have a manual TLS configuration or an Auto-TLS enabled for the Hadoop cluster. For both cases, NetBackup needs a root CA certificate from the administrator.

The root CA certificate from the Hadoop cluster can validate the certificates for all nodes and allow NetBackup to run the backup and restore process in case of the secure (SSL) cluster. This root CA certificate is a bundle of certificates that has been issued to all such nodes.

Certificate from root CA must be configured under `ECA_TRUST_STORE_PATH` in case of self-signed, third party CA or Local/Intermediate CA environments. For example: In case of AUTO-TLS enabled Cloudera environments, you can typically find the root CA file named with `cm-auto-global_cacerts.pem` at path `/var/lib/cloudera-scm-agent/agent-cert`. For more details, refer Cloudera documentation.

Table 2-4 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, or Nutanix AHV, this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_TRUST_STORE_PATH = Path to the external CA certificate` For example: `c:\rootCA.pem` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
Equivalent UI property	No equivalent exists.

Chapter 3

Cohesity Sheltered Harbor solution workflow

This chapter includes the following topics:

How to use NetBackup solution for Sheltered Harbor

This section contains detailed information on how to perform the data vaulting operation using NetBackup Sheltered Harbor solution.

To perform the configuration, registration, backup, and restore operations, use the `nbshvault` command.

After you carry out the configuration, registration, backup, or restore operations, see the following directory paths to view the logs:

Windows: `NetBackup_install_path\NetBackup\logs\nbshvault`

UNIX: `/usr/openv/netbackup/logs/nbshvault`

Note: The log directory is not created by default. To do so, you need to run the `mklogdir` command on the NetBackup client.

The `nbshvault` command can be executed by non-root user by running it along with `nbcmdrun` command. Only non-interactive mode is supported when it is executed using `nbcmdrun` command.

Following are the two methods to perform configuration, registration, backup, or restore operations:

- Use interactive mode
  See "Perform data vaulting using interactive mode" on page 29.

  Note: Use the interactive mode in case you want to run the NetBackup Sheltered Harbor solution manually.

- Use non-interactive mode
  See "Perform data vaulting using non-interactive mode" on page 37.

  Note: To perform operation using non-interactive mode, JSON files are required to pass the input to the NetBackup Sheltered Harbor solution.

Perform data vaulting using interactive mode

Interactive mode of command lets you perform configure, backup, and restore data operations. To perform these data vaulting operations, you need to manually enter the values to run the Sheltered Harbor solution. Interactive mode is performed manually and cannot be used for automated daily data vaulting process.

To understand how the data vaulting operations are performed using the interactive mode, see the following:

Configure operation

Configuration operation is the first step to be done to configure the Sheltered Harbor solution.

Note: Ensure that the configure and register operations are completed before you perform the backup or restore operations.

Use the following procedures to perform the configure operation:

To configure the Sheltered Harbor solution

1 Run either of the following commands on the command prompt:

- `nbshvault --configure`

- `nbshvault --configure [--config-dir` *`config-dir-path`*`]`

If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

2. Enter the Institution ID.
3. Enter the following logging information about the Sheltered Harbor solution:
   - Maximum log file size (default size is 10 MB).
     The Sheltered Harbor solution rotates the log when the log file size exceeds to the maximum log file size.
   - Verbose value (default value is 2).
     You need to specify the verbose value between 2 to 5 to see warning, and critical level message in the log file. To see the debug level messages, specify the verbose value as 6.
4. Enter the Sheltered Harbor license file path.

Note: Sheltered Harbor validates licenses of financial institutions every year. The license file needs to be provisioned on the NetBackup client where the Sheltered Harbor solution runs.

Note: Ensure that you have the read permissions to the license file to run the `nbshvault` command.

---

5. Enter monitoring log type such as **Live monitor** or **Stage monitor** to send an attestation message after successful data vaulting.
6. Select the solution type such as **Alta Solution for Sheltered Harbor** or **NetBackup Solution for Sheltered Harbor**.

Note: Alt Solution for Sheltered Harbor is the default option selected.

---

7 Enter the NetBackup API key path when you select the solution type as **NetBackup Solution for Sheltered Harbor**.

Note: You need to create NetBackup API key using NetBackup web UI beforehand with the required RBAC permissions. You must add the NetBackup API key in the text file with the following format <primary server name>:<NetBackup API key>.

Ensure that you have the read permissions to the API key path.

---

8 Enter the primary server backup policy.

Note: The storage unit value in the primary server backup policy needs to be configured with the immutable cloud storage bucket or with the storage lifecycle policy replicating the image to IRE domain on immutable storage.

---

9 Enter the following details for KMIP based KMS and Azure key vault:

Select KMIP based KMS or Azure Key Vault.

For example, (KMIP, Azure).

If you enter KMIP based KMS, do the following:

- Enter the KMS server name:
- Enter the KMIP port [5696 is default]:
- Enter the absolute path of certificate file:
- Enter the absolute path of private key file:
- Enter the absolute path of CA certificate file:
- Enter the envelope private encryption key ID:
- Enter the envelope public encryption key ID:
- Enter the envelope private sign key ID:
- Enter the envelope public sign key ID:

If you enter Azure Key Vault, do the following:

- Enter Vault URI of Azure Key Vault:
- Enter an authentication option for Azure Key Vault:
  - 1. Managed Identity
  - 2. Service principal with a Client Secret [1,2] : 2

- Enter Azure client ID:
- Enter Azure tenant ID:
- Enter Azure Client secret path: /root/sharbor/storage/tsp/jsonf.json
- Do you want to use online certificate status protocol (OCSP) [y,n] [n is default]:
- Enter Azure envelope private encryption key ID: SH
- Enter Azure envelope public encryption key ID: SH
- Enter Azure envelope private sign key ID: SH
- Enter Azure envelope public sign key ID: SH

10 If you want to configure the solution, the following information is asked:

- Enter the proxy server hostname or IP address
- Enter the proxy port [3128 is default]
- Enter the proxy type
  - HTTP
  - HTTPS
  - SOCKS5 [1,2,3] [1 is default]
- Do you want to configure proxy server authentication ? [y,n] (n):
- Enter the username:
- Enter the absolute path of the proxy server password file

The following example shows the configuration operation:

```
[root@sh-lin-5 bin]# nbshvault --configure
This command configures Sheltered Harbor solution in NetBackup.
Do you want to continue ? [y,n] (y) y
Enter the institution ID: XXXXXXX
===== Logging =====
Enter the maximum log file size in MB [10 MB is default]: 10
Enter the verbose value [2 is default]: 10
===== Solution Type =====
Enter NetBackup Sheltered Harbor solution type
1.Alta™ Solution for Sheltered Harbor
2.NetBackup™ Solution for Sheltered Harbor [1,2] [1 is default] : 1
===== License =====
Enter the Sheltered Harbor license file path: ${PATH_TO_LICENSE_FILE}
===== Sheltered Harbor Monitoring Log Type =====
```

```
Enter monitoring log type for sending an attestation message after successful data vaulting
1.Live monitor
2.Stage monitor [1,2] [1 is default] : 2
===== NetBackup Artifact Information =====
Enter the primary server policy: ${POLICY_NAME}
===== KMS =====
Do you want to configure KMIP based KMS or Azure Key Vault ? [KMIP, Azure]
[KMIP is default] : KMIP
Enter the KMS server name: xxxxyyyyyzzzz.com
Enter the KMIP port [5696 is default]:
Enter the absolute path of certificate file: ${path}/cert_chain.pem
Enter the absolute path of private key file: ${path}/key.pem
Enter the absolute path of CA certificate file: /${path}/cacerts.pem
Enter the envelope private encryption key ID: 4777666545678909876 5fghjklhhg6768900hj
Enter the envelope public encryption key ID: hhyvvgfrrykj68894048746326532thg
Enter the envelope private sign key ID: 4777666545678909876 5fghjklhhg6768900hj
Enter the envelope public sign key ID: hhyvvgfrrykj68894048746326532thg
===== PROXY SERVER DETAILS =====
Do you want to configure proxy server for outbound external connections ? [y,n] (n) : y
Enter the proxy server hostname or IP address  : ${PROXY_IP_ADD}
Enter the proxy port  [3128 is default] : 3128
Enter the proxy type
1. HTTP
2. HTTPS
3. SOCKS5 [1,2,3] [1 is default] : 3
Do you want to configure proxy server authentication ? [y,n] (n) : y
Enter the username  : admin
Enter the absolute path of proxy server password file : ${PATH_TO_PROXY_FILE}
Configuration is saved successfully.
The requested operation is successfully completed.
```

Register institution

After configuration with the Sheltered Harbor solution, you must register the institution with the Sheltered Harbor monitoring log.

Note: Ensure that you have configured the Sheltered Harbor solution before you register the institution.

Use the following procedures to register the institution with the Sheltered Harbor monitoring log.

Registration procedure

1. Run either of the following commands on the command prompt:

   - `nbshvault --register`
   - `nbshvault --register [--config-dir` *`config-dir-path`*`]`

   If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

2. Enter the institution ID, and registration ID (provided by the Sheltered Harbor).

   The following example shows the register operation:

   ```
   nbshvault --register
   This operation generates private key and sends registration message
   to the Sheltered Harbor monitoring log.
   Do you want to continue? [y,n] (y) y
   Enter the institution ID:
   Enter the registration key provided by Sheltered Harbor:
   Institution ID is already registered.
   ```

   On successfully running the command, the following message is displayed on the console:

   ```
   Registration successful. Status: 'Institution' is
   registered successfully. Please use the same public/private key for
   attestation Message: On Boarding Created
   ```

Backup operation

Backup operation lets you back up the institution input data using interactive mode. Use the following procedures to perform the operation.

Backup procedure

1. Run either of the following commands:

   - `nbshvault -b | --backup`
   - `nbshvault -b | --backup [config-dir` *`config-dir-path`*`]`

If you have provided the `config-dir` option during configuration, you should use the the same option for the command as well.

2 Enter the Institution ID.

3 Enter the input storage path and transfer storage path.

Note: Use the `--force` option along with `--backup` when the backup JSON file is provided to continue with backup even though attestation for the last backup has failed.

The backup and attest command options cannot run in parallel as they process the same set of files.

The following example shows the backup operation:

```
nbshvault -b
This command backs up the data as per the Sheltered Harbor
compliance specifications. Do you want to continue? [y,n] (y)
Enter the institution ID:
Enter the input storage path:
Enter the transfer storage path:
```

Restore operation

Restore operation in the Sheltered Harbor solution lets you decrypt the restored data files to its original state. The restore operation can be done using the following two methods:

- Archive retrieval
  Archive retrieval retrieves specified archive (encrypted volumes and a secure envelope) to recovery storage using BAR GUI or NetBackup web UI.
- Data restoration
  Data restoration process decrypts data and validates integrity of restored files. This can be done by restore operation using the interactive mode.

To perform restore operation, first you need to restore the data using the Backup Archive Restore (BAR) GUI or web UI to the recovery storage location. You can then perform the restore operation using the interactive mode.

Use the following procedure to perform the restore operation.

Restore procedure

1 Run either of the following commands on the command prompt:

- `nbshvault -r | --restore`

- `nbshvault -r | --restore [--config-dir config-dir-path]`

If you have provided the `config-dir` option during configuration, you should use the same option in the command.

2. Enter the institution ID.
3. Enter the recovery storage path and restored data storage path.

   The following example shows the restore operation:

```
nbshvault -r
This command performs data restoration as per the
Sheltered Harbor compliance specifications. Do you want to continue? [y,n] (y)
Enter the institution ID:
Enter the recovery storage path: /root/recovery_storage/
Enter the restored data storage path: /root/d4/
```

Attestation operation

The `nbshvault --attest` command option is used when the data vaulting to Alta Recovery Vault and IRE is completed but it failed to send an attestation message to the Sheltered Harbor monitoring log.

Use the following procedures to perform the attestation operation.

Attestation procedure

- Run either of the following commands on the command prompt to send the attestation message to complete the backup operation:
  - `nbshvault --attest`
  - `nbshvault --attest [config-dir config-dir-path]`

The command `nbshvault` can be executed by non-root RBAC user by running it along with 'nbcmdrun' command. Only non-interactive mode is supported when it is executed using `nbcmdrun` command.

Refer to the *NetBackup Command Reference Guide* for more information about `nbcmdrun` command.

Note: Run the `nbshvault --report` command option to fetch the backup keyword for attestation.

The backup and attest command options cannot run in parallel as they process the same set of files.

The following example shows the attest operation:

```
nbshvault --attest
Enter the institution ID: institution ID
Checking for any latest pending image for attestation
Skipping vaulting attestation as vaulting attestation is set to
false in input configuration JSON file.
```

Perform data vaulting using non-interactive mode

This section provides you the details on how to perform configuration, backup and restore data vaulting operations using JSON files provided as an input. The Non-interactive mode can be used only for automated daily data vaulting process.

To start the data vaulting operations using JSON files, you need to generate JSON templates that provided as an input. To generate those JSON templates, refer the following instruction:

To perform data vaulting using non-interactive mode

- Run the following command on the command prompt to generate JSON templates:
  - `nbshvault --generate-template -path <path>`

  Note: You must specify the path where you want to create the JSON file templates and you have the required access to the path.

  NetBackup Sheltered Harbor solution supports data vaulting by generating the following JSON file templates:
  - `config.json`
  - `backup.json`
  - `restore.json`

  Note: You must provide the correct JSON formatted file while performing the data vaulting operation. If you are using Windows, you need to specify the double backslash (\\) in the path.

  For example: `E:\\SH_Part2\\input_storge`

Configuration operation

Configuration operation is performed using `config.json`. You have to manually run the compliance solution with the configure option. It is a one-time activity. The

NetBackup Sheltered Harbor solution runs the daily vaulting process to backup and restore (periodic or on demand) using already configured data.

The compliance solution stores the configuration locally on disk file and uses the same during the backup or restore operations.

Configure the Sheltered Harbor solution using the JSON file as input:

Configure using non-interactive mode

- Run either of the following commands on the command prompt:
  - `nbshvault --configure filename`
  - `nbshvault --configure filename [--config-dir config-dir-path]`

If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

Note: To allow solution to use a well-known CA certificate while communicating with Sheltered Harbor Monitoring log, Use value 'NA" for a key "ca_cert_path" in input configuration JSON file.

On successful execution of the command, the Sheltered Harbor solution is configured.

The following example shows the configure operation:

```
nbshvault --configure /root/config.json
Configuration is saved successfully.
The requested operation was successfully complete
```

Register Institution

After configuration with the Sheltered Harbor solution, you must register the institution with the Sheltered Harbor monitoring log.

Note: Ensure that you have configured the Sheltered Harbor solution before you register the institution.

Carry out the following step to perform backup operation to register the institution with the Sheltered Harbor monitoring log

Register using non-interactive mode

- Run either of the following commands on the command prompt:
  - `nbshvault --register -i institution _ID -reg-key registration_key`

- `nbshvault –register -i institution ID -reg-key registration key [--config-dir config-dir-path]`

If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

This command option lets you provide the institution ID and registration key.

Once the command is run successfully, the institution is registered to the Sheltered Harbor monitoring log

The following example shows the register operation:

```
nbshvault --register -i 021000100 -reg-key d176dab5706b34cb699eadd07f6b77
<Institution ID> is already registered
```

Backup Operation

A backup operation is performed using the `backup.json` file. The `backup.json` file contains the information related to backup such as input storage path, and transfer storage path.

Carry out the following step to perform backup operation

Backup using non-interactive mode

- Run either of the following commands to backup data to Alta Recovery Vault:
  - `nbshvault -b filename --force | --backup filename --force`
  - `nbshvault -b | --backup filename [--config-dir config-dir-path] --force`

If you have provided the `config-dir` option during configuration, you should use the `config-dir` option in the command as well.

Note: Use --force option along with --backup when provided Backup Json file, to continue taking backup even if attestation for last backup is failed.

Note: The backup and attest command options cannot run in parallel as they processes same set of files.

On successful execution of the command, the data is backed up on an immutable storage.

The following example shows the backup operation:

```
nbshvault -b /root/NEW_TEMP/backup.json
Performing license validation.
```

```
License validation is successful.
Checking for any latest pending image for attestation
No latest pending image found for attestation.
Started backup operation
Backup operation is successful.
The requested operation was successfully completed
```

Restore Operation

Restore operation in the NetBackup Sheltered Harbor solution lets you decrypt the restored data files to its original state. The Restore operation cab be done using the following two methods:

- Archive retrieval
  Archive retrieval retrieves specified archive (encrypted volumes and a secure envelope) to recovery storage using BAR GUI or NetBackup web UI.
- Data restoration
  Data restoration process decrypts data and validates integrity of restored files. This can be done by restore operation using the non-interactive mode.

A restore operation is performed using restore.json. The restore.json file contains the information related to restore such as recovery storage path, and restored data storage path.

To perform restore operation, you first need to download the data from the BAR GUI and save it to the recovery storage location.

Carry out the following steps to perform restore operation.

Restore using non-interactive mode

- Run either of the following commands to restore the data:
  - `nbshvault -r | --restore filename`
  - `nbshvault -r | --restore filename [--config-dir config-dir-path]`

If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

On successful execution of the command, the data is restored to a restored data storage path on your system.

The following example shows the restore operation:

```
nbshvault -r /root/NEW_TEMP/restore.json
Restore operation is successful.
The requested operation was successfully completed.
```

Attestation Operation

The nhshvault`--attest` command option is used when the data vaulting is completed to Alta Recovery Vault but failed to send attestation message to Sheltered Harbor monitoring log.

Use the following procedure to perform the attestation operation.

Attestation using non-interactive mode

- Run either of the following command on the command prompt to send the attestation message to complete the backup operation:
  - `nbshvault --attest [-k keyword] | [-i institution ID]`
  - `nbshvault --attest [-k keyword] | [-i institution ID] [--config-dir config-dir-path]`

If you have provided the config-dir option during configuration, you should use the config-dir option in the command as well.

Note: Run the nbshvault`--report`command option to get the backup keyword for attestation.

Note: The backup and attest command options cannot run in parallel as they processes same set of files.

The following examples show how you can perform the attest operation either using backup keyword or institution ID:

Example 1: Use backup keyword

```
nbshvault --attest -k keyword
Checking for any latest pending image for attestation
Attesting pending image for the latest backup process
The requested operation was successfully completed.
```

Example 2: Use institution ID

```
nbshvault --attest -i institution ID
Checking for any latest pending image for attestation
Attesting pending image for the latest backup process
The requested operation was successfully completed
```

About key management services (KMS)

The NetBackup Sheltered Harbor solution encrypts and decrypts the data encryption key with the help of cloud KMS (CKMS) or on-premises KMS (KMIP based).

To start configuration with the NetBackup Sheltered Harbor solution, it is required to configure cloud KMS or on-premises KMS. You need to create KMS key pair for encryption, decryption, signing and sign verification.

Note: NetBackup KMS cannot be used for configuring the Sheltered Harbor solution.

The NetBackup Sheltered Harbor solution supports the following KMS:

- CKMS: Supports the Azure key vault
- EKMS: Supports Thales cipherTrust manager and utimaco ESKM

To know more about CKMS and EKMS, refer to EKMS document.

About configuration recovery in NetBackup solution for Sheltered Harbor

It is recommended to take periodic backups of the NetBackup Sheltered Harbor solution configuration present on NetBackup client. In case of a disaster, the configuration can be recovered and used once the client is up and running. You need to ensure that the periodic backup takes place on the specified directories where the NetBackup Sheltered Harbor solution configuration is stored.

You need to run periodic backups on the following directories of NetBackup client with the Sheltered Harbor solution:

Windows: `InstallPath\var\nbshvault`

UNIX: `/usr/openv/var/nbshvault`

Viewing operation details

To generate reports

Generate reports to view data vaulting operation details.

Run one of the following commands to show the report of past backup or restore jobs:

- `nbshvault --report | --report -n`

- `nbshvault --report | --report -n [--config-dir config-dir-path]`

If you have provided the `config-dir` option during configuration, you should use the `config-dir` option in the command as well.

By default, it shows 10 records.

- `nbshvault –report -n number`

This command option is recommended if you need to specify the number of records you want to see at the end of the command.

The following table contains the information on the data vaulting operation reports:

Table 3-1 Reports

Field	Description
Timestamp	The time stamp in UTC format.
Institution ID	The institution ID.
Operation	The operations to use, either backup or restore.
Backup Keyword	The backup keyword that helps to search for specific backup files or folder that are used at the time of recovery.
Step	Shows the details of ongoing operation.
Step Status	The record step status whether it is started, completed or failed for the ongoing operations.
Completion Status	The final operation status - failed or successful
Backup ID	The backup ID.
Status message	The final message or exit code at the completion of the operation. If you encounter any error, the exit code message is displayed.

To run show-config operation

This section provides information on how to view the configuration option.

To view the configuration operation

- Run one of the following commands:
  - `nbshvault --show-config -i institution ID`

- `nbshvault --show-config -i institution ID [--config-dir config-dir-path]`

If you have provided the `config-dir` option during configuration, you should use the `config-dir` option in the command as well.

Chapter 4

Glossary

This chapter includes the following topics:

Glossary terms for NetBackup Sheltered Harbor solution

The following are the terms used for NetBackup Sheltered Harbor solution:

Table 4-1 Glossary terms

Terms	Definitions
Archive volume	An encrypted file resulting from the encryption of the compressed volumes. A set of archive volumes for the same financial entity and business date constitutes an archive.
Archive	A set of archive volume files containing encrypted account data files as the financial entity stores the data securely in the data vault.
Archive generation	The daily data vaulting process that generates the archive by compressing and consolidating the account data files and corresponding hash files into the set of compressed volume. The archive gets encrypted to yield the archive volumes.
Archive repository	A sub-process of the daily data vaulting process to securely store the archive volumes and secure envelope in the data vault.
Attestation message	A daily message is sent to the monitoring log during vaulting attestation as a proof of a successful archive repository for the financial entity.
Cryptographic material	A set of cryptographic parameters used for validation and decryption of the archive volumes to restore the account data files during a NetBackup Sheltered Harbor solution event.

Table 4-1 Glossary terms *(continued)*

Terms	Definitions
Data restoration	The process of extraction of the account data files from the archive volumes and validating the integrity of the extracted files.
Data vaulting	A daily process of extracting the data from the originating institution and storing in the immutable storage.
Encryption keys	Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable.
Immutable vault	The property of the data vault, which guarantees that the content of the vault cannot be erased or modified in any worse-case scenario.
Input data	A set of files that is provided by the originating institution to the daily process to perform archive generation and secure repository for a financial Institution. The fileset that includes the manifest, account data files, and corresponding hash files.