Hewlett Packard Enterprise

HPE Data Protector 9.07 Deduplication

Introducing Backup to Disk devices and deduplication

Table of contents

Summary

This document describes how HPE Data Protector integrates with Backup to Disk devices and deduplication. By supporting deduplication, several new concepts are introduced to Data Protector, including a new device type, the Backup to Disk device, and four interface types: the HPE StoreOnce Software deduplication, the HPE StoreOnce Backup System, Smart Cache, and the EMC Data Domain Boost. Backup to Disk devices and deduplication are both discussed in detail in this document.

Backup to Disk devices are devices that back up data to a physical storage disk and support multi-host configurations. They support different backends such as the HP StoreOnce Software deduplication, the StoreOnce Backup system, Smart Cache, or the EMC Data Domain Boost. This document also describes the basic principles behind *deduplication technology.*

Data Protector supports the following deduplication backends:

- *HPE Data Protector Software deduplication* provides the ability to deploy target-side deduplication on virtually any industry-standard hardware, offers greater flexibility than existing solutions as it can be deployed in a wider range of hardware set-ups, and provides enterprise-class scalability.

  Because of the way Data Protector makes use of the extremely efficient HPE StoreOnce engine, Data Protector software deduplication uses memory very efficiently. As a result, you can deploy deduplication on application or backup servers without lowering application performance. Data Protector software deduplication can even be deployed on a virtual machine. In addition, Data Protector software deduplication delivers very high throughput.

- *HPE StoreOnce Backup system* devices are disk to disk (D2D) backup devices which support deduplication.

- *Smart Cache* devices are backup to disk devices that enable non-staged recovery from VMware backups.

- *EMC Data Domain Boost* devices are D2D backup devices which support deduplication.

For full details on supported systems, see the latest HPE Data Protector support matrices at http://support.openview.hp.com/selfsolve/manuals. For general Data Protector procedures, see the *HPE Data Protector Help*.

Overview

The Backup to Disk device (abbreviated to B2D throughout this document), together with a deduplication interface, uses deduplication technology to back up data to disk. Data deduplication is a data compression technology which reduces the size of the backed up data by not backing up duplicate data.

The deduplication process splits the data stream into manageable chunks (or blocks) of data. The contents of these data chunks are then compared to each other. If identical chunks are found, they are replaced by a pointer to a unique chunk. In other words, if 20 identical chunks are found, only one unique chunk is retained (and backed up) and the other 19 are replaced by pointers. The backed up data is written to a disk-based destination device called a *deduplication store*. When a restore operation is done, the unique chunk is duplicated and inserted in the correct position as identified by the pointer. With deduplication-type backup and restore operations, the restore process is sometimes referred to as *rehydration* of the backed up data.

There are several deduplication technologies available in the marketplace. They are generally grouped into hardware-based and software-based solutions. These solutions can be further sub-grouped, for example, into file-level (single-instancing) or block-level deduplication.

About StoreOnce software deduplication

Data Protector's StoreOnce software deduplication offers a software-based, block-level deduplication solution.

When using StoreOnce software deduplication, note the following:

- Deduplication backs up to disk-based devices only. It cannot be used with removable media such as tape drives or libraries.
- Because Data Protector uses a software-only approach to deduplication (that is, when using StoreOnce software deduplication), no specific hardware is required other than standard hard disks to store the backed up data.

- In the deduplication process, duplicate data is deleted, leaving only one copy of the data to be stored, along with reference links to the unique copy. Deduplication is able to reduce the required storage capacity since only the unique data is stored.
- StoreOnce software deduplication uses hash-based chunking technology to split the data stream into sizeable chunks of data.
- Specifying a *Backup To Disk* device with the StoreOnce Software deduplication interface in the backup specification tells Data Protector to do a deduplication-type backup.

When to use deduplication

Typically, you would use a B2D device with data deduplication support when backing up an e-mail filesystem which may contain 100 instances of the same 1 MB graphic file attachment. If the system is backed up using a conventional backup technique, all 100 instances of the attachment are backed up. This requires approximately 100 MB of storage space. However, if the backup is done through a B2D device deduplication support, only one instance of the attachment is actually stored. All other instances are referenced to the unique stored copy. In this example, the deduplication ratio is approximately 100 to 1. Although this example is referred to as *file-level deduplication*, it serves to demonstrate the benefits of B2D devices and deduplication.

Other points to consider when deciding to use deduplication technology:

- Some data is not a good deduplication candidate! Data that is automatically created by a computer does not deduplicate well, for example, database files. Photos, video, audio, imaging, seismic data are all examples of data that do not deduplicate very well.
- Do not compress data before deduplicating it. It will impact on the deduplication ratio (see also Deduplication ratio) and is unnecessary as compression is done following deduplication.
- Do not encrypt data before deduplicating it. This produces a deduplication ratio 1:1, basically, no deduplication.

Advantages of B2D devices and deduplication

Generally, data deduplication increases the speed of the backup service as a whole and reduces overall storage costs. Data deduplication significantly reduces the amount of required disk storage space. Because data deduplication is a disk-based system, restore service levels are significantly higher and tape (or other media) handling errors are reduced. Additional benefits of deduplication include:

- Data deduplication is more appropriate with large volumes of data.
- Data Protector uses well-proven deduplication algorithms to guarantee data integrity (StoreOnce software deduplication uses deduplication technology developed by HPE Labs for HPE StoreOnce Backup Systems. These systems use hardware-based deduplication. For more information about HPE StoreOnce products, see For more information).
- Disk-to-disk (D2D) storage with deduplication is rapidly becoming the preferred method for backup and recovery in both local and remote applications.
- The total cost of recovery for duplication-enabled D2D systems is significantly lower than with tape-based systems. Data deduplication backups can provide considerable capacity and cost savings compared to conventional disk backup technologies.

Deduplication performance

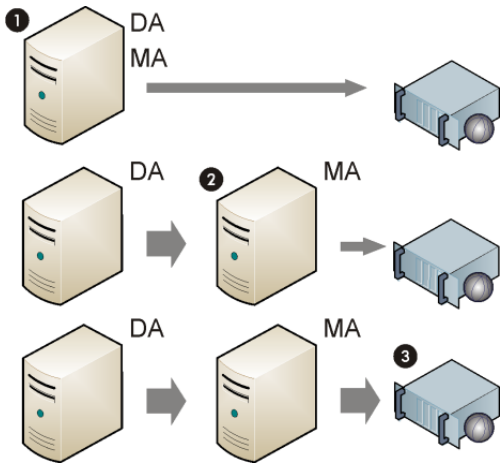
There are many factors that can affect deduplication performance. These include hardware and network speed, how the storage disk is set up, the size of the store, the deduplication ratio of the data, and how many concurrent backups are running. Using multiple streams can significantly improve backup performance. The number of parallel streams reading and writing data to a store is limited by the target device. For performance-related details, see Appendix D: System requirements and performance.

How deduplication integrates with Data Protector

Data Protector supports various deduplication setups:

- *Source-side* deduplication - data is deduplicated at the source (the backed up system).
- *Server-side* deduplication - data is deduplicated on the Media Agent system (the gateway).
- *Target-side* deduplication - data is deduplicated on the target device (StoreOnce Backup system or StoreOnce Software system).

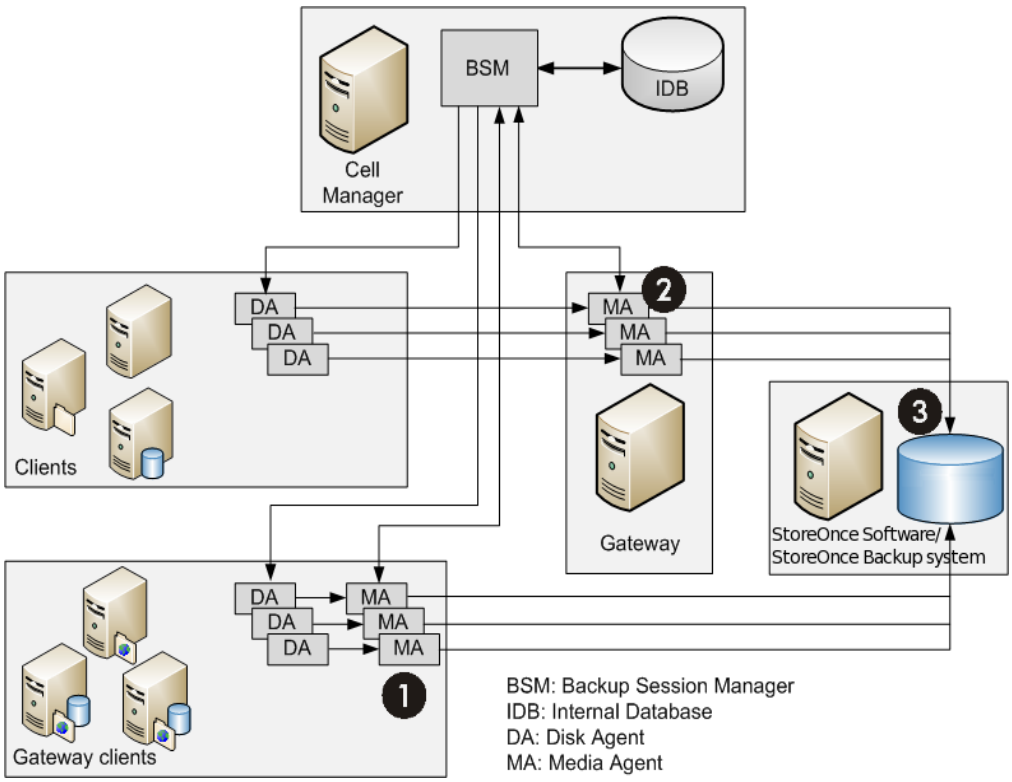
Figure 1: Deduplication setups



(1) Source-side deduplication
(2) Server-side deduplication on a dedicated Media Agent client
(3) Target-side deduplication on the device

Data deduplication integrates with Data Protector as shown in Figure 2. Data is read by the Disk Agents on the clients and written by the Media Agents (the gateways) to the target device. The role of *gateway clients* is discussed in Gateways. Deduplication can be performed at various stages as shown in Figure 1. The B2D device configuration is stored in the IDB.

Figure 2: How deduplication integrates with Data Protector



Source-side deduplication

With source-side deduplication (1), a Media Agent is installed together with the Disk Agent on the client that is backed up and thus the client becomes a gateway (a *source-side gateway*). The deduplication is performed by the Media Agent on the client itself so only deduplicated data is sent to the target device, thereby reducing the overall network traffic. The number of concurrent streams is limited by load balancing settings. Once a Media Agent finishes the backup of local objects, a new Media Agent is started on the next client system.

Note that the backed up system must support deduplication. For details, see the support matrices.

Server-side deduplication

With server-side deduplication (2), deduplication is performed on a separate Media Agent client (a gateway) by the Media Agent. This reduces the load on the backed up system and on the target device, but does not reduce the amount of network traffic between the Disk Agent and Media Agent.

Note that the Media Agent client must support deduplication. For details, see the support matrices. Server-side deduplication enables you to deduplicate data from clients on which deduplication is not supported locally.

Target-side deduplication

The deduplication process takes place on the target device (3). It receives data to be backed from Media Agents installed on clients (gateways).

Target-side deduplication using the StoreOnce Software system

The StoreOnce Software deduplication system then writes the deduplicated data to the StoreOnce library (this is the physical store and is sometimes referred to as the deduplication store).

The StoreOnce software deduplication system allows connections from several Media Agents, locally or remotely. It also provides synchronization mechanisms to enable multiple Media Agents to work with the StoreOnce library at the same time. The Media Agent reads or writes data in terms of object versions to or from the StoreOnce library. Each object version is represented as an item in the StoreOnce library. To optimize deduplication performance, Disk Agent concurrency is not supported (this means, one Disk Agent *talks* to one Media Agent – there is no multiplexing of streams). An example configuration showing a basic local and remote office deployment is given in Example configuration using a B2D device.

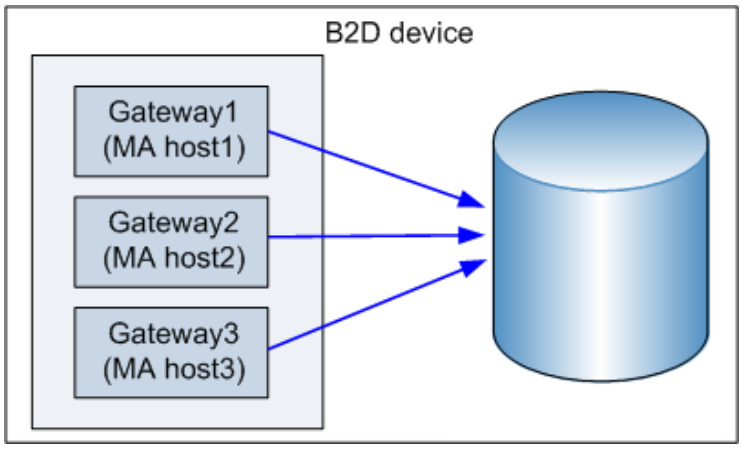
Target-side deduplication using the StoreOnce backup system device

The deduplication process looks from the Data Protector perspective very similar to target-side deduplication using the StoreOnce software system. However, there is no separate StoreOnce software deduplication system and the deduplication takes place on the StoreOnce Backup system device itself.

Backup to Disk device concepts

A Backup to Disk (B2D) device backs up data to a physical storage disk. The B2D device supports multi-host configurations. This means that a single physical storage disk can be accessed through multiple hosts called *gateways*. Each gateway represents a Data Protector client with the Media Agent component installed. A B2D device is a logical device and consists of gateways and a store. Figure 3 shows the relationship between a generic B2D device with multiple gateways and a store.

Figure 3: B2D device (logical view)

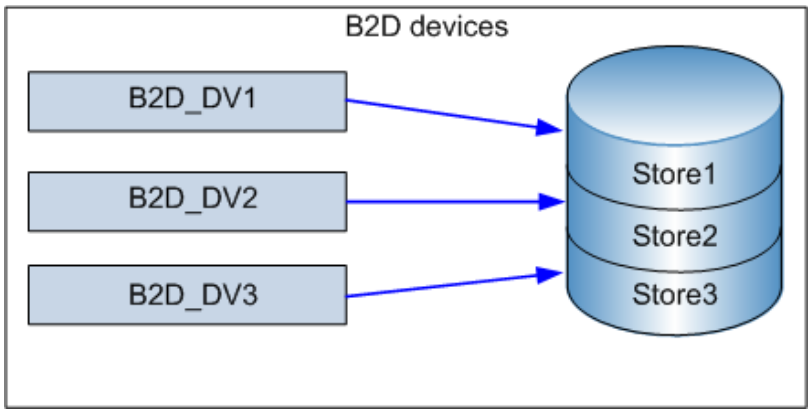


The physical storage can also be divided into individual stores representing specific storage sections, similar to partitioning a hard disk. A store is represented by a network path and is used by the backup application. These parameters, along with any other device-configuration information, are stored in the device configuration in the IDB.

Each individual store on the physical storage disk can be accessed by one B2D device only. However, several B2D devices can access different stores on the same physical storage.

Figure 4 shows three individual B2D devices accessing three individual stores on the same physical disk.

Figure 4: Multiple B2D devices accessing multiple stores on the same physical storage (physical view)



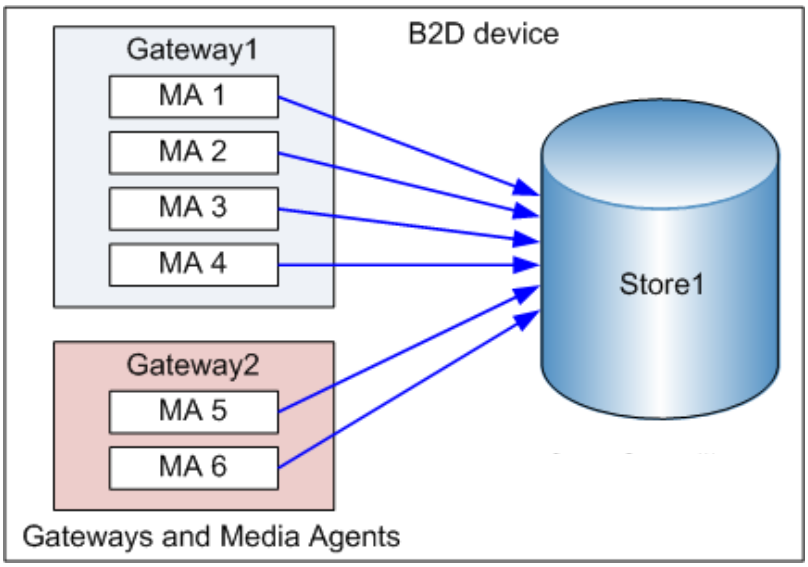
When configuring a B2D device, note the following:

- It is possible to configure multiple stores on a single deduplication-server node. These stores share resources, such as, CPU, memory, disk I/O, and the number of connections per deduplication system. However, each store represents its own deduplication domain. Deduplication does not happen across different stores.
- Each store must have its own dedicated B2D device configured. It is not possible to have two stores configured to the same B2D device.
- Each B2D device must use a store exclusively. Accessing the same store by more than one B2D device is not supported.

B2D device operation

The B2D device type is similar in structure to other library-based devices, that is, the device is comparable to a library and the gateway is comparable to a drive in the library. However, the operation is significantly different. Whereas library drives could be considered as *unique* because they could only be accessed by one Media Agent at a certain point in time, gateways behave differently and allow more flexibility. Each gateway represents a host on which multiple Media Agents can be started simultaneously, either in single or multiple sessions.

Figure 5: Gateways and Media Agents (physical view)



The number of Media Agents that can be started on a specific gateway is defined by:

- Gateway limits. Each B2D gateway is limited to a maximum number of parallel streams. This limit is specified in the GUI.

- Connection limits to the store. Each B2D device is limited to a maximum number of connections per store. This limit is specified in the GUI. If the value is left unchecked, Data Protector uses the maximum available.
- The physical connection limits of the physical storage disk. This value is retrieved from the physical store (see below).
- Depending on the current operation, each Session Manager attempts to balance the number of Media Agents on a gateway with regards to the following input parameters:
  - The number of objects being backed up
  - Object location
  - Physical connection limits.

The physical connection limit (the maximum number physically possible) is verified during the session. The value entered in the GUI is checked against the number of available connections. If the value entered exceeds the physical limit, the physical limit is used. The physical connection limit cannot be configured in the GUI. (Note: To use the maximum number, uncheck the option). When no data connections are active, the physical connection limit is 100. Data connections made after this limit is reached will not succeed.

If a large physical store has been partitioned into smaller stores (Store1, Store2, Store3 as previous), each of these stores has a limit to the number of connections.

Device locking

The purpose of locking is to ensure that only one system at a time communicates with a device that is shared between several systems. With B2D devices, certain connection limits must be obeyed. These connection limits are the maximum number of parallel streams per gateway and the maximum number of connections per store. Data Protector keeps a lock count for both these resources. When the limit is reached, the lock is denied. If the locking request is successful, the lock counts for both the gateway and the store are increased. When the gateway is unlocked, the lock counts are decreased. This ensures that B2D connection limits are considered *Cell Manager-wide* and not just during a specific session.

Object consolidation

To accommodate gateway and gateway/store/device connection limits, object copy and consolidation functionality makes sure that:

- When B2D devices are used as sources, at least one connection is available for object copy and at least *n* connections for object consolidation – where *n* is the number of source media used for consolidation (see the next paragraph for details).
- When B2D devices are used as targets, at least *m* connections must be available – where *m* is the minimum device setting in the copy/consolidation specification. If other types of devices are used in parallel, the CSM (Copy and Consolidation Session Manager) tries to balance them such that the minimum setting is reached, otherwise it terminates the session.

When consolidating backed up data (full and incremental backups), make sure there are enough available connections to the store. This is easier to explain by considering an example consolidation session of six incrementals. In this case, the number of connections = 1 (Full) + 6 (Incr) + 1 (target) = 8 connections. It is recommended to run a weekly consolidation session for between 6 to 10 incrementals.

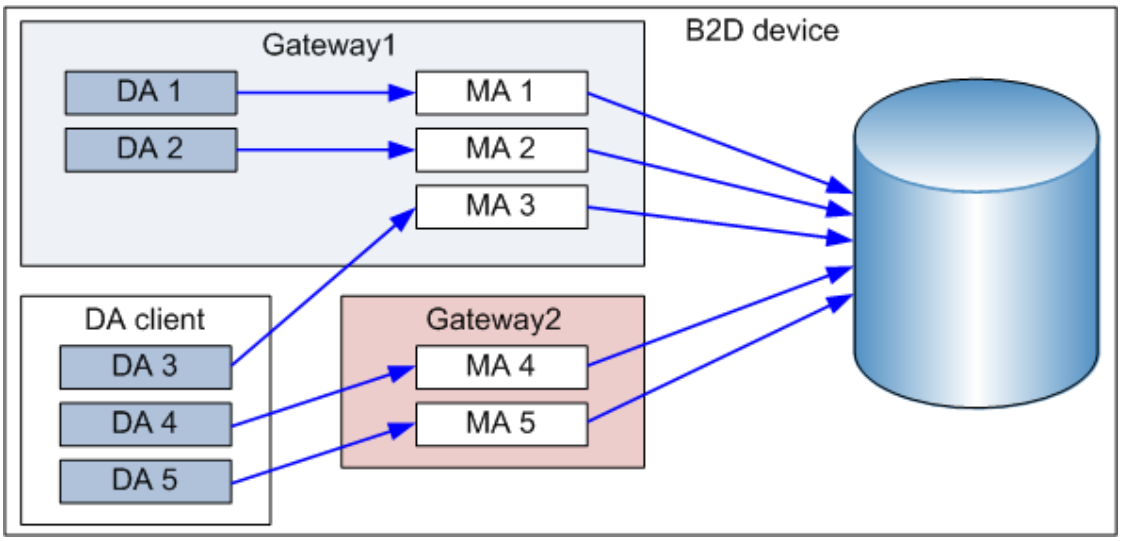
Backing up data using B2D devices

Making a backup to a B2D device is similar to backing up to tape-based devices. The notable differences are that the Session Manager dynamically spawns Media Agents on defined gateways and the Media Agent communicates with the devices through a device-specific API.

The following is an example of a backup session utilizing one B2D device with two gateways (Gateway1 and Gateway2). Five objects are being backed up (DA 1 ... DA 5), two objects are local to first gateway and three are remote to both gateways. The number of connections to the physical storage is six. The backup specification is configured with:

- Load balancing (Max) parameter set to 5 (meaning that up to five Media Agents can be used during this session)
- The connection limit for the B2D device is set to 10.
- The connection limit for both gateways is 5.

Figure 6: Sample backup configuration using two gateways (local and remote objects)



The Session Manager dynamically starts five Media Agents based on the above configuration. Since there are two gateways involved, the five Media Agents are distributed between the two gateways. The load balancing algorithm distributes the Disk Agents between the Media Agents such that Disk Agents local to Gateway1 are assigned to Media Agents on that gateway. Other Disk Agents are load-balanced between the two gateways since they are remote to all Media Agents.

When creating a backup specification, a B2D device can be selected as a target. It is also possible to select specific gateways. If a B2D device is selected as a target device, then all gateways will be chosen during the backup process using up-to-date device configuration information. However, this only works for load-balanced backups. When configuring a static backup (non-load balanced), you can only assign each object to a gateway and not to a B2D device.

B2D devices use a special data format for fast read/write access and to improve the deduplication ratio. The format splits the metadata from the actual data to be backed up. The data format is automatically set when you select a B2D device and is only used for B2D devices.

Gateways

Backup to Disk (B2D) devices must be configured to access pre-defined gateways. A gateway, or rather a *gateway client*, is a client with the Media Agent component installed (the client must be a 64-bit system, see below). It can be backed up as with any other client in the cell. Gateways are identified by a unique name. A gateway name includes a network pathname which points the device to the physical store. The default naming convention is similar to file libraries: *DeviceName*_gw*number*. Gateways are selected from a drop-down list in the GUI. Clients which cannot act as gateways are not listed.

Gateway connectivity can be verified (checked) to make sure the device is able to communicate with the gateway. If the gateway is unavailable for any reason, an error state is displayed. Additionally, gateway properties and features include:

- Gateway properties such as the gateway name and advanced options can be modified in the Gateway Properties dialog. The properties of multiple gateways can be modified simultaneously (see **Error! Reference source not ound.**).
- Gateways can be enabled or disabled. To enable or disable a gateway, right-click the gateway you want to enable or disable in the Device list and select Enable Gateways or Disable Gateways as appropriate.
- The Media Agent component can only be installed on 64-bit client systems. This means that if a client is to be designated as a gateway, it must be a 64-bit system (see Supported platforms).
- Each gateway represents a host on which multiple Media Agents can be started at the same time, either in a single session or in multiple sessions. For this reason, a gateway is sometimes referred to as a Media Agent host.
- If you are familiar with library-based devices, the B2D device is comparable to a library and the gateway is comparable to a drive in the library.

Source-side gateways

You can also configure one *source-side* gateway per device. This (virtual) gateway is automatically expanded on the backed up system if source-side deduplication is enabled. The default naming convention for these gateways is *DeviceName*_Source_side.

StoreOnce library (deduplication store)

The StoreOnce library (or deduplication store), is the physical storage disk used by the StoreOnce software deduplication interface (StoreOnce software deduplication uses HPE StoreOnce Backup System technology developed by HPE Labs). The supported capacity of the physical disk is 20 TB (of deduplicated data). Typically, with a deduplication ratio of say 20:1, this is equivalent to backing up 400 TB of data. If multiple stores are used, the total supported capacity is still 20 TB. To view the properties of a store, use the CLI commands (see Appendix A: StoreOnceSoftware utility).

One StoreOnce software deduplication system can host multiple deduplication stores providing the stores share the same root directory. Although Data Protector supports up to 32 stores per volume, best performance (with respect to the deduplication ratio) is achieved with one store only. Configuring the deduplication store is completed in a single stage (see **Error! Reference source not found.**).

Deleting expired backup data from the deduplication store

Periodically, Data Protector automatically triggers a cleanup session to delete backed up data residing in the physical store. Several methods are employed for removing unprotected data (for details, see Addition to omnimm):

- Manual removal of unprotected B2D backup objects

  Data Protector builds a list of unprotected backed-up objects residing in the store. Data Protector first removes them from the store and then deletes the media (object's) information from the Data Protector database. Note that removing media from the store does not free-up disk space; it merely instructs the store to obsolete the data.
- Automatic removal of unprotected B2D backup objects

  This method does the same as the above but is performed automatically by Data Protector at regular intervals. The interval can be configured in the global options file.
- Immediate removal when a slot is deleted

  Deleting a slot deletes the slot from the IDB, deletes the object in the slot, and the slot itself is removed from the store. This is the same action as recycling and deleting.

Removing unprotected B2D backup objects deletes the associated slots immediately. Deleting items does not free-up disk space immediately. During the next housekeeping job, expired files and unreferenced chunks are deleted, and possibly freeing up some disk space.

NOTE: Redundant data is data that is no longer referenced in the store. With expired data, the protection date has expired.

Clearing redundant data from the deduplication store

Data Protector provides a space-management (housekeeping) utility to optimize storage space. The housekeeping utility is started by default and runs in the background.

A data chunk becomes redundant when it is no longer referenced by the indexing table. Data is not deleted automatically from the store. This only occurs when the housekeeping utility runs and frees-up disk space.

StoreOnce Software Store robustness

StoreOnce software deduplication has a built-in mechanism to verify the integrity of the store. To minimize or prevent data loss, take note of the following:

- Use an uninterruptible power supply (UPS). It enhances the fault tolerance of the StoreOnce Software deduplication system. A UPS allows your computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges.
- The store must be configured as a RAID array. Due to the directory structure of deduplication stores, if one disk corrupts, the whole store becomes unusable. Hardware RAID is preferable.
- For critical data, it is recommended to do object copy operations from the deduplication store to a tape. Do not write to the store while backing it up.

Deduplication statistics

For backup sessions using deduplication, Data Protector displays the backup statistics after each object version is complete, for example:

```
Source-side Deduplication Statistics for dd2.company.com:/C "C:".
       Using device: "b2d_Source_side [GW 13148:3:649335383]@dd2.company.com":
              Mbytes Total: ..................        35 MB
              Mbytes Written to Disk: .......         1 MB
              Deduplication Ratio: ..........       35.0 : 1
```

The statistics includes:

- `The type of the deduplication (source-side, target-side, and server-side)`
- `Information about the device.`
- `Mbytes Total`: The original size of the object version (the data to be backed up).
- `Mbytes Written to Disk`: The actual size written to the disk after deduplication. (If less than 1 MB, 1 MB is displayed).
- `Deduplication Ratio`: The 'Mbytes Total' divided by the 'Mbytes Written to Disk'. (See notes below.)

When interpreting the deduplication ratio, note the following:

- If the value for 'Mbytes Written to Disk' is less than 1 MB, it is rounded to 1 MB (otherwise, the calculation produces an unrealistic result).
- Typically, you can expect a deduplication ratio of the order 10 - 20:1. Ignore erroneous ratios (for example, 4435:1). This can occur when the denominator (Mbytes Written to Disk) is extremely small.

The ratio displayed in the backup statistics applies to the current session. The ratio displayed in the CLI, applies to the store as a whole.

Deduplication ratio

The storage capacity saved by using deduplication is typically expressed as a ratio. The sum of all pre-deduplicated backup data is compared with the actual amount of storage the deduplicated data requires. For example, a ratio of 10:1 means that 10 times more data is stored than there would be if deduplication was not used.

The most significant factors affecting the deduplication ratio are:

- Data retention period.
- The amount of changes between backups.
- File size: small files may result in a low deduplication ratio.

However, many factors influence how much storage is saved in your specific environment. The ratio is reported in the summary screen (after adding a device), in the Devices context (**Devices** > **Stores**), and in the backup statistics following a backup operation (for a typical output, see Deduplication statistics).

HPE recommends configuring the B2D device to use a block size of 256 KB to achieve higher deduplication ratios.

Limitations

- Data deduplication is not suitable for archiving of data.
- StoreOnceSoftware Agent is not supported in cluster environment.
- It is not supported for more than one B2D device to access the same store. This means that each B2D device must be configured to a dedicated store. Do not configure a second device to use the same store.
- If the number of connections required for consolidating backed up data (full and incremental backups) exceeds the maximum number of connections, the restore chain which could not be consolidated, terminates. See also Object consolidation.
- Disaster recovery is supported on Disk Agent clients with local gateways. To perform the disaster recovery on a Disk Agent client with a local gateway, you must select the **Use Original Network Settings** option in the Disaster Recovery settings.
- Object mirroring is not supported with source-side deduplication.
- Automated media copy is not supported for B2D devices.

- When you enable replication between B2D devices, you must set the maximum number of connections per store on the selected destination device to a number greater than or equal to the maximum limit on load balancing configured in the backup specification.
- You cannot select source-side gateways for object consolidation. For full backups, Data Protector automatically selects another gateway. For incremental backups, you need to select another gateway manually. The gateway must belong to the same B2D device as the source-side gateway.
- You cannot select source-side gateways for object copy. You can either:
  - Replace the read source device with a non-source-side gateway manually. The gateway must belong to the same B2D device as the source-side gateway.
  - In the Properties window of a non-source-side gateway, go to the Policies tab and select **Gateway may be used as source gateway for object copy**. Data Protector will automatically replace the source-side gateway with this gateway.
- When you enable encrypted control communication, exclusions are not supported. Once the cell member running the StoreOnceSoftware daemon is secured, the daemon will handle only secured connections.
- The StoreOnceSoftware service/daemon must be restarted manually after encrypted control communication is enabled for the system (cell member) where it runs.
- Source-side deduplication backup to StoreOnce Backup system devices configured with Fiber Channel (FC) can be performed on only those systems that are connected to FC. Therefore, before performing this backup, you must ensure that the systems meet the following requirements:
    - Data Protector Disk Agent is installed.
    - Data Protector Media Agent is installed.
    - Fiber Channel connection is configured.

  During backup, you can use the Systems ready for source-side deduplication option to filter out systems that do not support the source-side deduplication. However, this option does not filter out systems that do not have the FC connection, which is one of requirements for performing the source-side deduplication backup to StoreOnce Backup system devices configured with FC.

  To verify whether systems have the FC connection, click Check to validate the Gateways, while adding the StoreOnce Backup system device.
- The devices selected for replication must be capable of replication.
- The source and target device types that are selected for replication must be the same.
- Within the StoreOnce library, the source and target devices must belong to different stores.
- The source device must be configured in at least one backup specification.
- For StoreOnce Backup system or Data Domain Boost devices, replication to devices configured with Fiber Channel (FC) is not supported. Target devices must always be configured with IP addresses.
- When performing an interactive replication on Data Domain devices, only one session at the time can be selected for replication.
- The same version of the Data Domain OS (DDOS) must be installed on the source and destination Data Domain devices. For more information, see your Data Domain documentation.
- Replication to target device configured with the Fiber Channel address is not supported.

Installation

This section provides an overview of the main installation tasks and specific requirements when installing the StoreOnce Software Deduplication component.

Prerequisites

Make sure that the HPE Data Protector 9.00 Cell Manager, user interface client, and Installation Server are installed on supported systems.

For an overview of supported platforms, see Supported platforms. For details, see the latest HPE Data Protector support matrices at http://support.openview.hp.com/selfsolve/manuals. See the *HPE Data Protector Installation and Licensing Guide* on how to install Data Protector in various architectures.

Firewall configuration

Ensure that the following ports are open for incoming connections:

- `5555/tcp` – on all Data Protector clients (this is a prerequisite for the general Data Protector installation procedure) and on the StoreOnce library
- `9387/tcp` – command port (for StoreOnce Software systems and StoreOnce Backup systems, see also Appendix C: Omnirc option)
- `9388/tcp` – data port (for StoreOnce Software systems and StoreOnce Backup systems, see also Appendix C: Omnirc option).

Ports 9387 and 9388 must be open in a firewall separating the target device from any gateways. (Windows systems: Ports are opened during the installation process, UNIX systems: Ports must be manually opened.) For details on Data Protector ports, see the *HPE Data Protector Help* index: "port range".

Installation procedure

Install the `Data Protector Media Agent` or the `NDMP Media Agent` component on all systems that will become gateways, including the clients on which source-side deduplication will be enabled.

For instructions, see the *HPE Data Protector Installation Guide*. For a detailed list of supported operating system versions, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Additional steps for StoreOnce Software deduplication

Install the Data Protector StoreOnce Software Deduplication component on the system which will host the StoreOnce store.

The StoreOnce Software Deduplication component can be installed locally or remotely.

Remote installation of Data Protector StoreOnce Software Deduplication component

1. Connect to any client with the Data Protector `User Interface` component.
2. Open the Data Protector GUI and, in the Context List, select **Clients**.
3. Add the Data Protector `StoreOnce Software Deduplication` component to a backup client:
   - If the backup client is not part of the Data Protector cell, use the Data Protector **Add Clients** functionality.
   - If the backup client is already part of the Data Protector cell, use the Data Protector **Add Components** functionality.

Following successful installation, the StoreOnce software deduplication component is listed in the Installed components list.

Before you can use StoreOnce software deduplication, the root directory of the stores must be configured. To find out how to do this, see **Error! Reference source not found.**.

Local installation of Data Protector StoreOnce Software Deduplication component

Windows systems:
During a local installation of Data Protector, select the `StoreOnce Software Deduplication` component in the Components list.

Linux systems:
Run `omnisetup.sh –install StoreOnceSoftware`.

Setting up the StoreOnceSoftware service/daemon

Windows systems:
Following successful installation, the StoreOnceSoftware executable is started as a service (see Services tab in the Task Manager). The service name is `Data Protector StoreOnceSoftware`, the description is `StoreOnce Software Deduplication`, and the startup type is automatic.

Linux systems:
To install the StoreOnceSoftware daemon such that it starts automatically after a system restart, copy the file `StoreOnceSoftwared` to the `/etc/init.d` directory and include it in startup scripts. The daemon can also be started or stopped manually using the commands:

```
/opt/omni/lbin/StoreOnceSoftwared start
```

and

```
/opt/omni/lbin/StoreOnceSoftwared stop
```

Removing the StoreOnce Software Deduplication component from the system automatically stops the process and removes the file `StoreOnceSoftwared` from the `/etc/init.d/` directory.

The installed directory structure

Windows systems:

The installation component includes the following files:

Filename	File location
`StoreOnceSoftware.exe`	*`Data_Protector_home`*`\bin`
`system.db`	*`Data_Protector_program_data`*`\Config\client\StoreOnceSoftware`

Linux systems:

Following successful installation, StoreOnceSoftware is started as a background process (daemon). Following a restart, it can be started automatically.

The installation component includes the following files:

Filename	File location
`StoreOnceSoftware`	`/opt/omni/lbin`
`StoreOnceSoftwared`	`/etc/init.d/` `/opt/omni/lbin`
`system.db`	`/etc/opt/omni/client/StoreOnceSoftware`

Additional steps for Data Domain Boost devices

- To support replication, DDOS version 5.2 and later is required.
- To support reporting deduplication statistics during replication, DDOS version 5.3 and later is required.
- To support replication between Data Domain devices, virtual synthetics must be enabled on the Data Domain devices.
    - Using ssh, connect to the Data Domain devices and run the following command:

      ```
      ddboost option set virtual-synthetics enabled
      ```

Licensing

B2D device licensing uses the capacity-based licensing (similar to file library licensing). During the session, the Media Agent gathers statistical information from the physical store (that is, the deduplicated data in the deduplication store) and sends it to the Session Manager, which in turn updates the licensing database. When a B2D device is deleted or modified in the IDB, the licensing database is updated. The B2D device requires a capacity-based *Advanced Backup to Disk* LTU which is available as follows (the used capacity is based on the usage of deduplicated data on disk):

- B7038AA – 1 TB
- B7038BA – 10 TB
- B7038CA – 100 TB

For more information about capacity-based licensing, see the *HPE Data Protector Installation and Licensing Guide.*

Configuration

This section includes an example environment and configuration procedures.

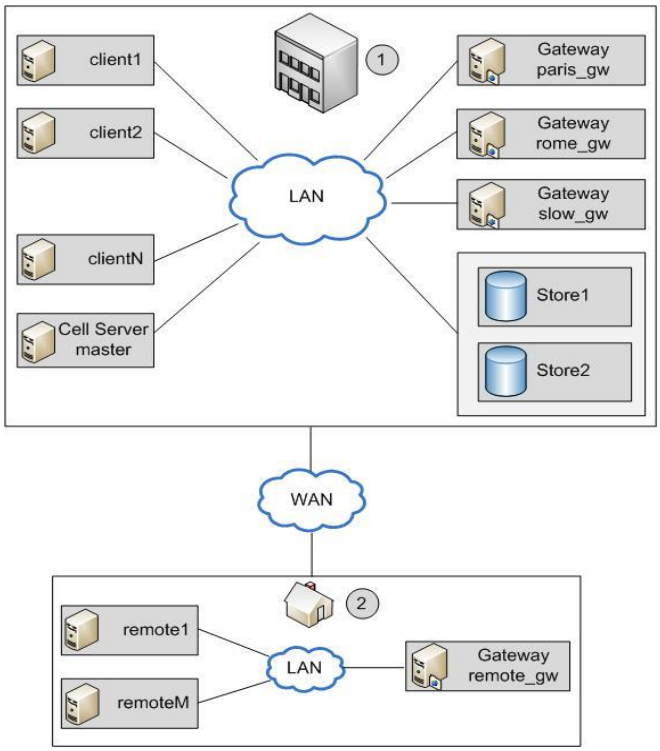
Multi-interface Support

Data Protector provides multi-interface support; both an IP and a FC connection can lead to the same Catalyst or Boost store. Data Protector supports IP as well as a fiber channel connection to the same Catalyst / DDBoost store without the need to configure a separate store. The store is accessible simultaneously over both interfaces. For example, sometimes a single Catalyst / DDBoost store can be accessed by local clients over fiber channel for faster backup while remote clients can access the same store over the WAN for slower backup. The configuration steps are provided in the Adding a B2D device section.

Example configuration using a B2D device

The following provides a typical usage model of a central office/remote office configuration.

Figure 7: Deployment example within a central office/ remote office environment



Item	Description
1	Central office. This LAN is located in the central office. It is connected to the LAN in the remote office over a WAN.
2	Remote office. This LAN is located in the remote office.

The Data Protector Cell Manager is installed in the central office on the host *master*. There are several clients in the central office: *client1* to *clientN* (non-gateway clients), *paris_gw*, *rome_gw*, and *slow_gw* (gateway clients). Additionally, two object stores (*Store1* and *Store2*) are configured in the central office.

The remote office includes clients *remote1* to *remoteM* and *remote_gw*. All clients in the remote office are part of the same Data Protector cell as the clients in the central office. The remote office is connected to central office over a slow WAN network.

NOTE: Gateways are simply clients with the Media Agent component installed. Think of them as *gateway clients*. For a client to become a gateway, it must be a 64-bit system (see Supported platforms).

When you configure a B2D device, you must specify certain parameters such as the name and location of the store, gateways, and network paths. In the above example, you want to use the store Store1 (which is accessed by StoreOnce software deduplication) for backup of clients in your environment. To do this, you configure the B2D device to use Store1 as the repository. You also decide that clients *paris_gw*, *rome_gw,* and *slow_gw* are to be used as gateways for other Data Protector clients in the central office. Additionally, note the following:

- Concurrency specifies a number of Disk Agents writing to the device in parallel. Multiple Disk Agents read data in parallel (from disks) to provide a constant data stream to the Media Agent. With StoreOnce software deduplication, Disk Agent concurrency for each Media Agent is set to 1 (this improves the deduplication ratio).
- Data Protector supports backup to non-encrypted as well as to encrypted stores. Encryption can be enabled at the time of the store creation. Note that once the store is created, you cannot change its state from encrypted to non-encrypted and vice versa.
- Only one store can be configured per device.

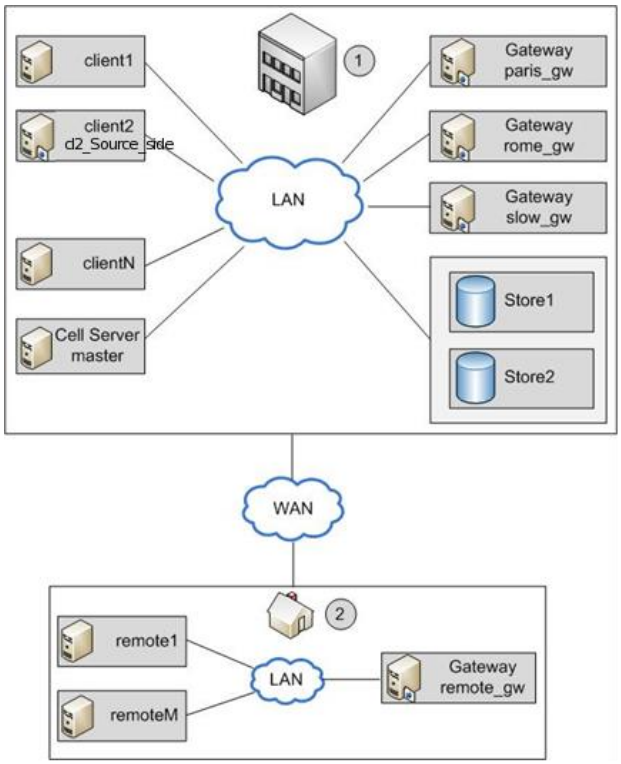
- Stores are represented by network paths (UNC) that contain information about the deduplication system and the store name. (Note: In the context of B2D devices, the deduplication system refers to name of the *hosting* machine where the deduplication store is located.)

Source-side deduplication

The above scenario is suitable if the amount of backed up data from individual clients is limited. However, to reduce the network traffic, you can configure source-side gateways.

For example, in our scenario, client2 is a system where a lot of data is duplicated but the system load is moderate. To reduce the network load, you can enable source-side deduplication for the B2D device. If you then also enable source-side deduplication in the backup specification for client2, a source-side gateway will be automatically created on client2 and the Media Agent will send only deduplicated data across the network.

Similarly, if you enable source-side deduplication for other clients, source-side gateways will be automatically created on those clients as well.



Adding a B2D device

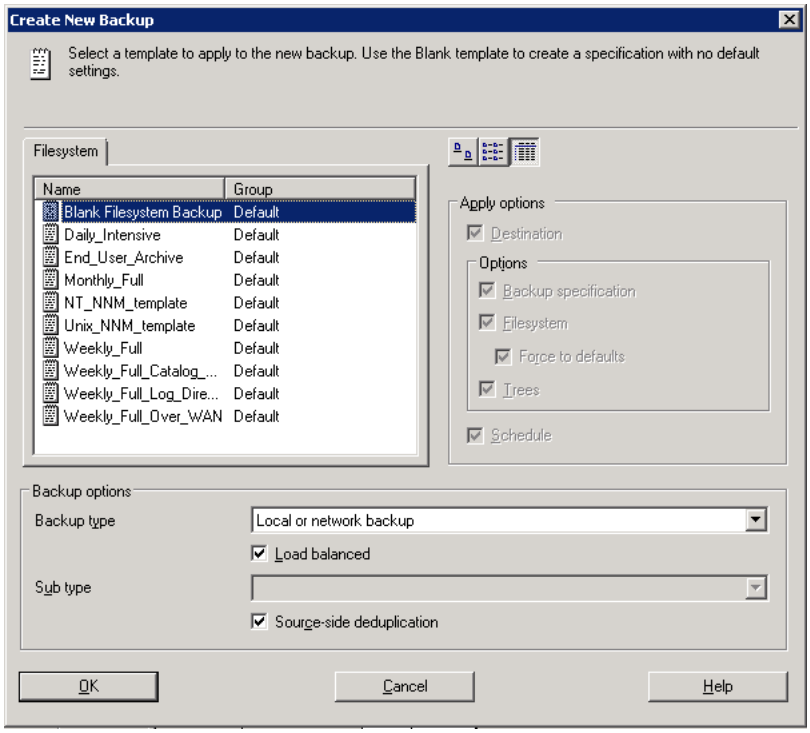
The procedure for adding a B2D device is similar to the procedure for adding device types. For more information, see *HPE Data Protector Online Help*, and *HPE Data Protector Administrator's Guide*.

Backup

Specifying a B2D device in the backup specification tells Data Protector to do a deduplication-type backup. The deduplication process runs in the background and the deduplicated data is written to the StoreOnce Software system or StoreOnce backup system.

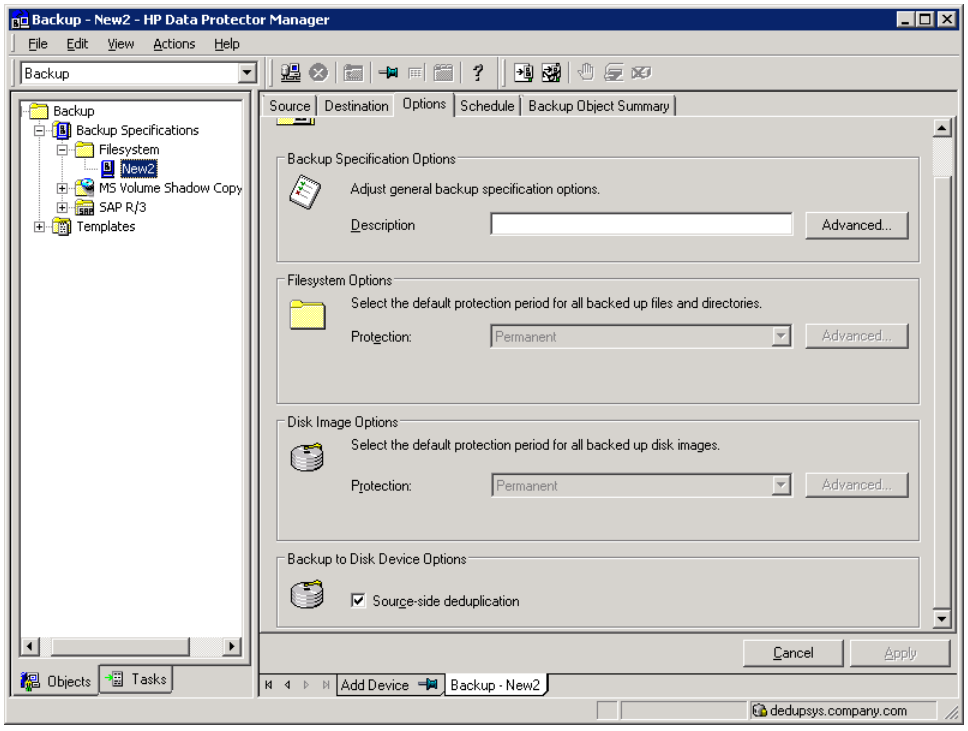
You make a data deduplication-type backup in the same way as a conventional backup:

1. Add a new B2D device (in this case, by specifying StoreOnce software deduplication or StoreOnce Backup system). See Adding a B2D device.
2. Create a backup specification which targets this device. See the *HPE Data Protector Help* index: "creating, backup specification". Optionally, to enable source-side deduplication, select the Source-side deduplication option when creating a backup specification.



When selecting backup objects in the Source page, Data Protector will shade all clients which do not have a source-side gateway configured. You can filter the list of clients by selecting **Source-side deduplication** in the Show drop-down list.

Alternatively, select the backup specification, open the Options pane and select **Source-side deduplication**.



3. In the Destination page, select a gateway to be used for backup. Click **Properties** to review and modify gateway options. Note that by specifying the option **Max. Number of Parallel Streams Per Gateway** you overwrite the value set during the device configuration.

NOTE: When source-side deduplication is selected, you can back up only objects from clients where source-side gateways are supported and select only devices with source-side gateways. If you deselect the option, Data

Protector will automatically select all gateways of the B2D devices instead of the source-side gateways and display a warning message.

IMPORTANT: If you enable source-side deduplication in existing backup specification, clients where source-side deduplication cannot be performed are deselected and not backed up.

Restore

You restore backed up data in the same way as with a conventional restore operation. Although, the background process of retrieving data from the deduplication store is significantly different when compared to conventional restore processes, there are no special tasks to be performed. The main operations in the retrieving process includes loading data to be restored into memory, reading reference information from index tables, and using this information to *rehydrate* the backed up data. See the *HPE Data Protector Help* index: "restore".

Source-side deduplication considerations

If the backup was performed with source-side deduplication enabled and the restore is performed to a client on which source-side gateways are not supported, an ordinary gateway will be used instead.

Troubleshooting

This section provides log and event reporting, warnings, diagnostics, and problem-solving information when using Data Protector B2D device integration. For general Data Protector troubleshooting information, see the *HPE Data Protector Troubleshooting Guide*.

Before you begin

- For general Data Protector limitations, as well as recognized issues and workarounds, see the *HPE Data Protector Product Announcements, Software Notes, and References*.
- For an up-to-date list of supported versions, platforms, and other information, see http://support.openview.hp.com/selfsolve/manuals.

Low disk space warning

To avoid running out of disk space where the stores reside, a warning message is written (Event Log on Windows systems or Syslog on Linux systems) when a pre-defined threshold is reached. The default value for the threshold is 10% of the store's capacity. The default value can be modified using the omnirc option (see Appendix C: Omnirc options related to B2D devices). The warning message is issued before any further read/write operations are done to the store, once per day, or if the StoreOnceSoftware utility is restarted. A warning is also shown in the backup session message at the beginning and at the end of the session. The low disk-space warning message is:

```
You are running out of disk space on Deduplication Store root directory:
[path]. The threshold x% is reached. Please free space or add more disks.
[warning].
```

Backup of the system.db file

The `system.db` database file contains root directory information and information about the stores. It is located under *`DataProtector_Program_Data`*`\OmniBack\Config\client\StoreOnceSoftware`. If this file is deleted or lost, the store and the backed up data cannot be accessed. To avoid this situation, every time a change is made to the database, a backup copy of the `system.db` file is made to `..\`*`Store_Root`*`\StoreOncelibrary\system.db.bak`. The `system.db` file can be restored by copying the backup file to the original location, renaming it, and restarting the StoreOnceSoftware utility.

Make sure that files under the root directory are protected (RAID or backup).

Problems

The following lists common problems and errors reported by the StoreOnceSoftware utility. Errors generally relate to the operating environment and the directory structure of the deduplication store.

Problem

Accessing the system.db file: The system.db file is inaccessible (for example, permission denied, or disk full).

The StoreOnceSoftware utility fails to find the root directory of the store.

Action

Change permissions, free disk space, or make the database accessible. The database file (`system.db`) contains an empty or no value for the root directory of the deduplication store. To recover the file, see Backup of the system.db file. To reconfigure the root directory to use another location, see `configure_store_root` in Appendix A: StoreOnceSoftware utility.

Problem

Accessing the system.db file: The system.db file in the root directory of the store is missing.

The StoreOnceSoftware utility fails to start.

Action

Restore or recreate the `system.db` file. See previous problem.

Problem

Starting stores: Store directory is inaccessible.

During startup of the store, an error is logged. The store cannot be accessed.

Action

Make the store's directory accessible, check permissions, and verify the root directory exists.

Problem

Starting stores: Store directory is missing.

Starting the store is successful, but no items are found.

Action

Restore the root directory and the stores below the root directory.

Problem

Starting stores: Store is dirty and cannot be recovered.

An error is logged. The store cannot be accessed.

Action

Restore the root directory and the stores below the root directory.

Problem

Stopping stores: Items are open (for example, backup or restore sessions are running).

Stopping the store reports an error. Store is closed in a *dirty* state (items, such as backup or restore, are open or running). Recovery may happen on next startup.

Action

Check that all operations are finished before stopping the StoreOnceSoftware utility.

Problem

Stopping stores: Housekeeping utility cannot be stopped.

An error is logged during shutdown. Recovery may happen on next startup.

Action

Check that all operations are finished and then stop the StoreOnceSoftware utility. Recovery may happen on next startup.

Problem

Warnings and error messages are logged into the Windows event log or Linux syslog by the StoreOnce Software service/daemon due to low disk space and memory

When the available disk space is low, a warning message will be logged and if the disk space is critically low, an error message will be logged and the service/daemon will reject further write operations. The read operations are not affected and restore is still possible.
When the system reaches 25% of free virtual memory left, a warning message is logged and when only 20% of free virtual memory left is left, an error message is logged and the service/daemon starts rejecting read and write operations.

Action

Free up system resources. The service/daemon will stop rejecting operations once the disk space or memory is freed.

Problem

Data Protector displays the warning »Store does not exist« and the backup session fails

When performing a backup session using a StoreOnce Backup system device, Data Protector displays a warning similar to the following and the session ends abnormally:
`[Warning] From: BSM@computer.company.com "CS2BackupTmp" Time: 6/18/2012 1:34:08 PM`
`Got error: " Store does not exist. " when contacting " DeviceName" B2D device!`
The issue can appear if the store was deleted on the B2D device or if the permissions for this store were modified.

Action

- Check if the store exists or if any of the permissions were modified for this store.
- If the store is set up correctly, check the device settings in Data Protector. Right-click the device, select **Properties** and in the Devices - Store and Gateways page check the **Client ID**.

Problem

Backup Size Soft Quota or Store Size Soft Quota are exceeded but Data Protector does not report any warnings.

This issue can appear because status updates on the B2D devices are performed in intervals, so the backup session can finish before the next B2D status update reports the exceeded quota.

Action

None. The next backup session will properly report the warnings.

Appendix A: StoreOnceSoftware utility

The StoreOnceSoftware utility is a service/daemon and maintenance tool for performing general administration tasks on the StoreOnce library (the deduplication store). Note: On Windows systems, the term *utility* refers to the `StoreOnceSoftware.exe` service. On Linux systems, `StoreOnceSoftwared` is a script which utilizes the `StoreOnceSoftware` CLI (the options are: `{start | stop | status}`).

Synopsis

```
StoreOnceSoftware --help | -hStoreOnceSoftware [--log_path=LogPath]
                     [--log_level={no_log|fatal|critical|error|warning|
                     notice|information|debug|tracing}]
StoreOnceSoftware --configure_store_root --path=RootDirectory [--force]
StoreOnceSoftware --create_store --name=StoreName
                     [--store_description=StoreDescription]
StoreOnceSoftware --modify_store --name=StoreName
                     [--store_description=StoreDescription]
StoreOnceSoftware --delete_store --name=StoreName [--force]
StoreOnceSoftware --start_store --name=StoreName
                     [--set_readonly=ON|OFF]
StoreOnceSoftware --stop_store --name=StoreName [--force]
StoreOnceSoftware --set_autostart=ON|OFF --name=StoreName
StoreOnceSoftware --list_stores [--name=StoreName]
StoreOnceSoftware --get_server_properties
StoreOnceSoftware --set_readonly=ON|OFF [--name=StoreName] [--force]
StoreOnceSoftware --daemon
```

NOTE: The same format is used for options on both, Windows and Linux platforms:

- `--option` or `--option=Value`

- The short notation only works for the help option: `--help` or `-h`

Note the following:

- Before any administrative store commands can be used, the StoreOnceSoftware utility must be running, otherwise, an error message is displayed.

  If the StoreOnceSoftware utility is *not* running and you do not specify a parameter, the following message is displayed: `The daemon is stopped`. Restart the utility with the command: `net start StoreOnceSoftware`.
- When starting the utility, you can define a path for logs and a logging-level with the options `--log_path` and `--log_level`.
- If the command-line option is not recognized (for example, the option is specified without the leading characters '-- '), the following message is displayed:
  `Unknown option specified: unknown_option`.
- You can use the omnirc command OB2DBGDIR for debugging purposes. Ensure that the path is in the correct format. For instance, OB2DBGDIR=/SOSLogs/.
- If you specify --log_path for logging, you must specify the path in the correct format. For instance, --log_path=/SOSLogs/postfix.txt.

Description

`--help | -h`

Displays a list of CLI options with descriptions.

`--configure_store_root --path=RootDirectory [--force]`

Configures the root directory of the store(s). The root directory must be configured before you can create a store. When StoreOnce software deduplication is first installed, it is running in a *non-configured* mode and cannot be used until the root directory of the store has been set. The option `--path` specifies the path to the root directory. The path must not be empty, must be a valid directory which already exists on the system, and not previously used as a store-root path. If successful, Data Protector displays the path in the CLI. If the root directory cannot be configured (there may be several reasons), you are prompted to stop/start the utility (daemon). Use the stop/start commands given below.

When the root directory is configured, Data Protector automatically creates the subdirectory `StoreOncelibrary` below the root directory.

Use the `--force` option to reconfigure the location of the root directory in cases where the actual data has been moved to another location. Make sure the data is already at the specified location before using the `--force` option (see below for details).

Once the root directory is configured, it cannot be reconfigured through the GUI. To move the store to a new, never previously used, location (in case of a disaster recovery or being unable to use the existing mount point), proceed as follows:

1. Stop the StoreOnceSoftware utility.

   Windows systems: Use `net stop StoreOnceSoftware` or use the Service Manager

   Linux systems: Use `/opt/omni/lbin/StoreOnceSoftwared stop`)
2. Manually move the data from the *`Old_Path`* to the *`New_Path`*. This means the subdirectory `StoreOncelibrary` and all its contents .
3. Run the command:
   `StoreOnceSoftware --configure_store_root --path=New_Path --force`
   (make sure *`New_Path`* includes the full path, for example, `--path=C:\Volumes\NewRoot`)
4. Start the StoreOnceSoftware utility.

   Windows systems: Use `net start StoreOnceSoftware` or use the Service Manager

   Linux systems: Use `/opt/omni/lbin/StoreOnceSoftwared start`)

See also Backup of the system.db file for information about the `system.db` file and the root directory, and **Error! Reference source not found.** for the GUI-based procedure to configuring the root directory.

`--log_path=`*`LogPath`*

Defines a path where logs are to be stored.

`--log_level={no_log | fatal | critical | error | warning | notice | information | debug | tracing}`

Defines the logging detail as defined by:

`no_log`	Logging is disabled (default value).
`fatal`	A fatal error. The application will most likely terminate. This is the highest severity.
`critical`	A critical error. The application might not be able to continue running successfully
`error`	A non-critical error. An operation did not complete successfully, but the application continues.
`warning`	A warning. An operation completed with an unexpected result.
`notice`	A notice, which is information with a higher severity.
`information`	An informational message, usually denoting the successful completion of an operation.
`debug`	A debugging message.
`tracing`	A tracing message. This is the lowest severity.

`--create_store --name=`*`StoreName`* `[--description=StoreDescription]`

Creates a deduplication store with the specified name. Depending on the success of the operation, one of the following messages is displayed:

- If successful: The store: *StoreName* has been created successfully.
- If the store exists: `The store `*`StoreName`*` has already been created.`
- If an error occurs: `Failed to create the store: `*`StoreName`*`.`
- If a name is not specified:
  `The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart`, require the name option.

`--modify_store --name=`*`StoreName`* `[--description=StoreDescription]`

Modifies the store with the specified name.

`--delete_store --name=`*`StoreName`* `[--force]`

Deletes the store with the given store name. The store is stopped before it is deleted.
If the `--force` option is used, the operation will try to close all the current activities, stop the store and then delete the store. One of the following messages is displayed:

- If successful: The store: *`StoreName`* `has been deleted successfully`.
- If an error occurs: `Failed to delete the store: `*`StoreName`*.
- If name of the store is not specified:
  `The options --start_store, --stop_store, --create_store, --delete_store and --set_autostart` require the `--name` option.

`--start_store --name=`*`StoreName`* `[--set_readonly=ON|OFF]`

Starts the store specified by the store name. Depending on the success of the operation, one of the following messages is displayed:

- If successful: `The Store `*`StoreName`*` has been successfully started.`
- If already started: `The store: `*`StoreName`*` has already been started.`
- If an error occurs: `Failed to start the store: `*`StoreName`*
- If a name is not specified:
  `The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart require the name option.`

`--stop_store --name=`*`StoreName`* `[--force]`

Stops the store specified by the store name. If the `--force` option is used, the store attempts to close all current connections and then stops the store. Depending on the success of the operation, one of the following messages is displayed:

- If successful: `The store: `*`StoreName`*` has been stopped successfully.`
- If already stopped: `The store: `*`StoreName`*` has already been stopped.`
- If an error occurs: `Failed to stop the store: `*`StoreName`*

- If a name is not specified:
  The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart require the --name option.

--set_autostart=ON|OFF --name=*StoreName*

Sets a store to be started automatically (ON) or not automatically started (OFF). Depending on the success of the operation, one of the following messages is displayed:

- If successful: Autostart option for the store *StoreName* successfully set to *ON/OFF*.
- If an error occurs: Failed to set Autostart option for store: *StoreName*
- If a name is not specified:
  The options --start_store, --stop_store, --create_store, and --set_autostart require the name option.

--list_stores

Displays a list of stores that are configured on the StoreOnce Software deduplication system. It includes the following information:

- Store Name
- Store ID
- Store Description
- Store Status
- Store Autostart status
- User Data Stored (original, not deduplicated data)
- Store Size on Disk (resulting, deduplicated data)
- Deduplication Ratio

Depending on the success of the operation, one of the following messages is displayed:

- If successful: Listing of the stores succeeded.
- If an error occurs: Failed to list the stores.
- If no stores can be identified: There are no stores in database.

--list_stores supports the use of the --name option, which lists only the information about the store specified with the --name option. The following is a typical output showing three stores:

```
C:\Users\Administrator>StoreOnceSoftware --list_stores

Store Name:             StoreOnceLibrary
Store Id:               1
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       1305 MB
Store Size on Disk:     770 MB
Deduplication Ratio:    1.7 : 1


Store Name:             Berlin_Store
Store Id:               2
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       20 MB
Store Size on Disk:     1530 KB
Deduplication Ratio:    13.7 : 1


Store Name:             Lisbon_Store
Store Id:               5
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       4549 MB
Store Size on Disk:     1174 MB
Deduplication Ratio:    3.9 : 1


Listing of the stores succeeded.
```

--get_server_properties

Displays a list of server/store related properties:

- Path and name of the root directory (Store Root:)
- Existing stores
- Available stores
- Space capacity

– Disk space free

```
C:\Users\Administrator>StoreOnceSoftware --get_server_properties

Store Root:             c:\StoreOnceRoot

Existing Stores:        3
Available Stores:       29
Disk Capacity:          49 GB
Disk Space Free:        29 GB

Listing of the daemon properties succeeded.
```

`--set_readonly=ON|OFF [--name=StoreName] [--force]`

Sets the store to read only or read/write mode. If no store name is given, the daemon is set to read only mode.
When the option is set to ON (read only mode), all ongoing write operations are allowed to finish and new ones are blocked. If the `--force` option is used, all ongoing write operations are closed.
When a store is in read only mode, you cannot modify stores using the `--modify` option.
When the daemon is in read only mode, you cannot create, modify or delete store, only starting or stopping a store is allowed.
The command will display the following messages:
On success:

- Daemon: `Read only option for daemon has been successfully set to ON/OFF.`
- Store: `Read only option for the store StoreName has been successfully set to ON/OFF.`

If an error occurs:

- Daemon: `Failed to set read only option for daemon.`
- Store: `Failed to set read only option for store StoreName.`

`--daemon`

Applies to Linux systems only. Run StoreOnceSoftware as a daemon for debugging purposes.

If the option `--name` is used in combination with non-valid options, the following message is displayed:

```
The option --name can only be specified with the --start_store,
--stop_store, --create_store, --delete_store, --set_autostart or the
--list_stores command.
```

The option `--description` can only be used when creating a store (`--create_store`).

Appendix B: Command line interface changes to support B2D devices

The following CLI command options are added or updated.

Addition to omnimm

Synopsis

```
omnimm -delete_unprotected_media [Library | -all]
```

Description

Manual removal of unprotected B2D backup objects

When invoked, Data Protector builds a list of unprotected backed-up objects residing in the B2D device. Data Protector first removes them from the store and then deletes the media information from the Data Protector database. Note that removing media from the store does not free-up disk space, it merely instructs the store to obsolete the data. You can optionally specify the name of the library. In this case only unprotected media from the specified library are deleted.

Description

Automatic removal of unprotected B2D backup objects

This method does the same as the above but is performed automatically by Data Protector at regular intervals. The interval can be configured in the global options file.

```
# DeleteUnprotectedMediaFreq=TimesPerDay
# default: 1
# limit: 1 <= DeleteUnprotectedMediaFreq <= 24
# If set to 1, operation is performed once per day (00:00),
# set to 2 two times per day (00:00,12:00), set to 3 three times
# per day (00:00, 08:00, 16:00),  set to 4 four  times  per  day
# (00:00, 06:00, 12:00, 18:00).  If maximum (24)  is  specified,
# operation will be started on every hour.
```

This functionality is implemented by the `omnitrig` command which calls `omnimm` at specified intervals.

Description

Immediate removal of objects when a slot is deleted

Deleting a slot deletes the slot from the IDB, deletes the media in the slot, and the slot itself is removed from the store. This is the same action as recycling and deleting. The commands are:

```
omnimm -recycle MediumID
omnimm -remove_slots Library Slot
```

Addition to omnidownload

Use this command and options to list devices, device information, and libraries.

Synopsis

```
omnidownload -list_devices
```

The following example shows a typical device-list output:

```
Device name          Host                 Device type              Pool Name
================================================================================
DeDup Device1_gw1    paris_gw.gateway.com    BackupToDisk StoreOnce    DeDup
Device1_MediaPool
DeDup Device1_gw2    rome_gw.gateway.com     BackupToDisk StoreOnce    DeDup
Device1_MediaPool
DeDup Device1_gw3    tercus.gateway.com      BackupToDisk StoreOnce    DeDup
Device1_MediaPool
```

Synopsis

```
omnidownload -dev_info
```

The following example shows a typical device-information output:

```
Device name                      Host             Device type             Pool Name
================================================================================
DeDup Device1                    device.box.host1    BackupToDisk StoreOnce
DeDup Device1_gw1 paris_gw.domain.com    StoreOnce    (in library) DeDup Device1_MediaPool
DeDup Device1_gw2 rome_gw.domain.com     StoreOnce    (in library) DeDup Device1_MediaPool
DeDup Device1_gw3 tercus.domain.com      StoreOnce    (in library) DeDup Device1_MediaPool
================================================================================
Together : 3 configured device[s].
```

Synopsis

```
omnidownload -list_libraries -detail
```

The following example shows a typical device-library output:

```
NAME "B2D Device"
DESCRIPTION ""
POLICY BackupToDisk
TYPE ObjectStore
REPOSITORY
"list_of_mediums"
DIRECTORY
```

```
 "\\d2d.domain.com\teamedStore" "<encoded_client_id>" "<encoded_password>"
MGMTCONSOLEURL ""
MAXCONNECTIONS #Num
B2DSOFTQUOTABACKUPSIZEGB #Num
B2DSOFTQUOTASTORESIZEGB #Num
B2DTEAMEDSTORE 1
B2DTEAMEDMEMBERS
"d2d.domain.com"
"d2d1.domain.com"
```

This output includes the following new parameters:

- B2DTEAMEDSTORE: Indicates whether the store is teamed.
- B2DTEAMEDMEMBERS: Lists the members of the teamed store.

omniupload

Use the `omniupload` command to upload information about a B2D device from an ASCII file to the Data Protector IDB. For command options, see the *HPE Data Protector Command Line Interface Reference*.

omnib2dinfo

Use the `omnib2dinfo` command to list details about the B2D devices. For a detailed description of the command, see the omnib2dinfo reference page in the *HPE Data Protector Command Line Interface Reference*.

Appendix C: Omnirc options related to B2D devices

The *omnirc* file is enhanced with additional options. Use this file to set such parameters as port number and disk-space threshold warnings. These changes apply to the client only.

`OB2_STOREONCESOFTWARE_COMMAND_PORT=`*`PortNumber`*
This option changes the port which is used for command communication between the Media Agent and the StoreOnceSoftware utility.
For example: `OB2_STOREONCESOFTWARE_COMMAND_PORT=12345`
Default: 9387

`OB2_STOREONCESOFTWARE_DATA_PORT=`*`PortNumber`*
This option changes the port which is used for data communication between the Media Agent and the StoreOnceSoftware utility.
For example: `OB2_STOREONCESOFTWARE_DATA_PORT=12346`
Default: 9388

`OB2_STOREONCESOFTWARE_SESSION_IDLE_TIMEOUT=`*`s`*
The StoreOnceSoftware daemon periodically checks for idle connections and terminates them. This option specifies the number of seconds of inactivity after which a connection is considered idle.
Default: 300 (Range: Minimum: 10)

`OB2_STOREONCESOFTWARE_DISK_SPACE_THRESHOLD=%`
This option is to set a threshold for the free disk space (see Low disk space warning).
Default: 10% (Range: 1% - 95%)

`OB2_STOREONCESOFTWARE_MINIMUM_DISK_SPACE=`*`n`*
This option controls the minimum disk space (in MB) the StoreOnceSoftware needs to reserve. If this minimum is reached, writing data to any stores will fail. Default: 1000 (Minimum: 500)

`OB2_STOREONCESOFTWARE_SSL_ENABLE=0|1`
Default: 1
This option enables or disables secure control communication between the client and the StoreOnce Software daemon. Note that even if the client on which StoreOnce Software daemon runs uses secure control communication, it will not be used if you set this option to 0.
After enabling secure communication, restart the StoreOnceSoftware daemon manually.

`OB2_STOREONCESOFTWARE_DISABLE_IPV6_LISTEN=0|1`
Default: 0

By default, the StoreOnce Software daemon listens on a dual-stack socket (IPv6 and IPv4 on the same port). If set to 1, IPv6 is disabled. This option applies to RPC and IpcServer listening ports.

`OB2D2D_COMMAND_PORT=`*`PortNumber`*
This option changes the port which is used for command communication between the Media Agent and the StoreOnce Backup system.
For example: `OB2D2D_COMMAND_PORT =12345`
Default: 9387

`OB2D2D_DATA_PORT=`*`PortNumber`*
This option changes the port which is used for data communication between the Media Agent and the StoreOnce Backup system utility.
For example: `OB2D2D_DATA_PORT=12346`
Default: 9388

`OB2D2D_NUM_OF_LBWTHREADS=`*`ThreadNum`*
Defines the number of threads used for the deduplication computation when deduplication performed on the Media Agent client. If you have a more powerful gateway, you can increase this number could to 8 threads. The option must be set on each gateway individually.
Default: 4

`OB2D2D_BANDWIDTH_BUFF_SIZE=`*`Size`*
Sets the size of the buffer when deduplication is performed on a Media Agent client. The default setting is appropriate when the Media Agent communicates with the D2D device through LAN. When a WAN network is used for communication, a more appropriate value is 20 MB. The option must be set on each gateway individually.
Default: 10 MB

Appendix D: System requirements and performance

This section lists the supported platforms and the minimum and recommended requirements for the StoreOnce Software deduplication system.

Supported platforms

Supported platforms for StoreOnce software deduplication component are:.

For latest information about the supported platforms, *see HPE Data Protector 9.0x Platform and Integration Support Matrix.*

- Windows Server 2008 R2 Enterprise (64-bit, x64)
- Windows Server 2008 (64-bit, x64)
- Oracle Enterprise Linux 6.4 (x64)
- CentOS 6.4 (x64)
- SUSE Linux Enterprise Server 10.x (64-bit, x86-64)
- SUSE Linux Enterprise Server 11.x (64-bit, x86-64)
- Red Hat Enterprise Linux (RHEL) 5.x (64-bit, x86-64)
- Red Hat Enterprise Linux (RHEL) 6.x (64-bit, x86-64)

StoreOnce Software Deduplication component can be installed on physical systems as well as on virtual machines. When choosing a virtual machine as your StoreOnce Software deduplication system, note that the performance of deduplication stores may be lower than expected.

NOTE: HPE recommends installing the StoreOnce Software Deduplication component to a system other than the Cell Manager.

For details on supported systems, see the latest HPE Data Protector support matrices at http://support.openview.hp.com/selfsolve/manuals. See the *HPE Data Protector Installation and Licensing Guide* on how to install Data Protector in various architectures.

StoreOnce Software deduplication system requirements

	CPU speed / number of cores[1] (dedicated to StoreOnce software)	**Physical memory**[2] (dedicated to StoreOnce software)	**Number of disks**[1] (dedicated to the store)
Minimum requirements (for 1 TB store)	2.8 GHz / 2 core	4 GB of RAM	1
Recommended requirements (for 10 TB store with 5 parallel connections)	2.8 GHz / 4-6 cores	6 GB of RAM	4 or more using RAID5
(1) For maximum performance, consider 1.3 cores, 0.8 disks, and additional 50 MB of RAM per parallel stream, and use a dedicated physical system as StoreOnce Software deduplication system. (2) 300 MB of RAM are needed for each 1 TB of store capacity.			

For data security and performance reasons, only local host filesystems are supported. This includes disks or volumes connected through SCSI, Fiber Channel, or iSCSI interfaces; NFS and CIFS are not supported. On Windows systems, only NTFS volumes are supported and on Linux systems, volumes with the 'ext4' or 'xfs' filesystems are supported.

HPE recommends RAID5 with a limited stripe size, which achieves good performance in conjunction with the ability to recover from a single disk failure.

Appendix E: Considerations for antivirus usage on the StoreOnce Software server

This section lists some of the considerations if you are using, or planning to use an antivirus product on the StoreOnce Software server.

- Scheduled scanning or real-time scanning of the StoreOnce Software root directory should not be performed because of its complex file structure.
- Scanning files in the folders that are part of the StoreOnce Software housekeeping process, can cause the StoreOnce Software to fail.
- Moving any files to the quarantine location, or deleting files when virus scanners identify a security risk inside the StoreOnce library folder structure, can corrupt the store, and make it unusable.

Recommendations

- Disable real-time virus scanning.
- Add the StoreOnce Software root directory to the "Exclude List" of the virus scanner.
- Regularly review the Store Root information by executing the `--get_server_properties` command.

Appendix F: Performance benchmarks for StoreOnce Catalyst and VTL devices

Environment:

- The StoreOnce deduplication system used is a B4210 single node physical device. A separate store is created for each test case.
- The Cell Manager is a Windows Server 2008 physical server
- The Disk Agent is a Windows Server 2008 server that has 500 GB of data to be backed up (in cases where data is sent to another server)
- The Media Agent is installed on three different servers with Windows, CentOS and HP-UX operating systems respectively.
- These tests were carried out using Data Protector patch bundle 9.04

			Disk Agent and Media Agent on the same server	**Disk Agent and Media Agent on different servers but within same network**
Backup Data	**Type**	**Gateway**	**Time (h:m:s)**	**Time (h:m:s)**
500 GB	Catalyst over Ethernet	Windows	1:32:0 (90.57 MB/s)	2:27:12 (56.61 MB/s)
500 GB	Catalyst over Fibre Channel		1:47:55 (77.22 MB/s)	2:34:17 (54.01 MB/s)
500 GB	VTL		1:41:24 (82.18 MB/s)	2:37:54 (52.77 MB/s)
500 GB	Catalyst over Ethernet	CentOS	58:30 (142.45 MB/s)	1:52:21 (74.17 MB/s)
500 GB	Catalyst over Fibre Channel		1:23:11 (100.18 MB/s)	1:52:25 (74.12 MB/s)
500 GB	VTL		1:45:13 (79.20 MB/s)	1:56:45 (71.37 MB/s)
500 GB	Catalyst over Ethernet	HP-UX	59:34 (139.89 MB/s)	3:0:7 (46.26 MB/s)
500 GB	Catalyst over Fibre Channel		1:53:42 (73.29 MB/s)	3:04:54 (45.06 MB/s)
500 GB	VTL		1:48:30 (76.80 MB/s)	3:43:34 (37.27 MB/s)

Appendix G: StoreOnce Catalyst Client Configurations for Catalyst over Fibre Channel

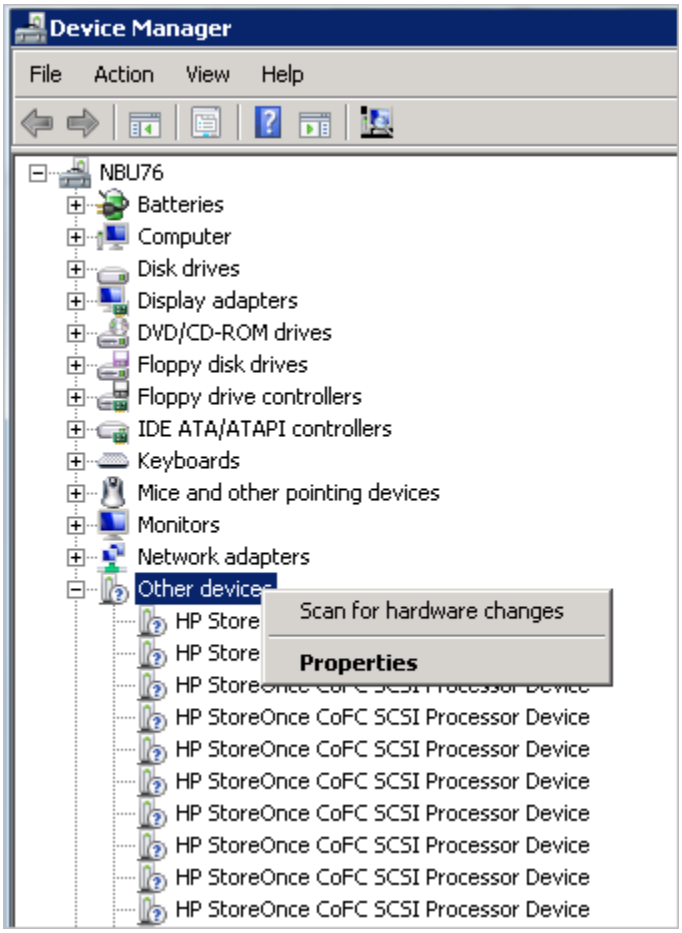
NOTE: The following information is not meant to be authoritative. For latest and most detailed information, refer to the *StoreOnce* documents.

Windows Clients

Administrator permissions are required to run Catalyst over Fibre Channel backups.

StoreOnce Catalyst over Fibre Channel presents a device type of **Processor**. After zoning the devices or changing the Number of Devices per Initiator Port, proceed as follows:

1. Go to **Windows Device Manager,** right-click **Other Devices**.
2. Select **Scan for hardware changes** to detect the new devices.



Linux Clients

StoreOnce Catalyst over Fibre Channel presents a device type of **Processor**. On Linux, the device files are created in `/dev/sg*`. By default, `/dev/sg*` devices are accessible only by the root users. For non-root user, provide the backup user permissions to access the device files using a Linux `udev` rule.

To create a `udev` rule, proceed as follows:

1. Create a `udev` file in the following location on each of the backup server:

   `/etc/udev/rules.d/70-cofc.rules`

2. Add the following rule to the file:

   ```
   KERNEL=="sg[0-9]*", ATTRS{vendor}=="HP*", ATTRS{model}=="StoreOnce CoFC*",
   ATTRS{rev}=="CAT1", GROUP="##CORRECT_USER_GROUP##"
   ```

   Where, `##CORRECT_USER_GROUP##` is replaced by the Linux user group, which will perform backups and restores. For example, `dba/oracle`.
3. Scan for device file changes to update the permissions.

   The `lsscsi --generic` command can be used to determine, which `/dev/sg*` device files belong to Catalyst over Fibre Channel.

AIX Clients

Prior to StoreOnce software 3.14 version, the StoreOnce Catalyst over Fibre Channel on AIX is available only by request.

NOTE: If you have a requirement for Catalyst over Fibre Channel on AIX 6.1 or 7.1 with StoreOnce versions below 3.14, contact BURA.Solutions@hp.com.

StoreOnce Catalyst over Fibre Channel presents a device type of **Sequential** on AIX. These device files are created in `/dev/rmt*` location. After zoning the devices or changing the Number of Devices per Initiator Port, proceed as follows:

1. Execute the `storeonce-cofc-passthrough-install.sh` script.

NOTE: This installation script is part of the StoreOnce software kit and not part of the HPE Data Protector.

2. Execute the `cfgmgr` command as a root user to scan the changes in the device file.
3. By default, `/dev/rmt*` device files are accessible by root users only. Running backups as a non-root user requires additional permissions.

HP-UX Clients

StoreOnce Catalyst over Fibre Channel presents a device type of **Processor**. On HP-UX, the device files are created in `/dev/pt/ptX` location.

After zoning the devices or changing the Number of Devices per Initiator Port, proceed as follows:

1. Scan for device file changes.
2. Execute the `ioscan -fnC /dev/pt` command as a root user.

   By default, `/dev/pt/ptX` devices are accessible only by the root users. For non-root user, provide the backup user permissions to access the device files using the `chmod o+rwx /dev/pt/pt*` command.
3. To get permissions for `/dev/pt/ptX` device files, use the Catalyst over Fibre Channel commands:

   ```
   /usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid |
   grep StoreOnce
   ```
4. Use `chmod o+rwx` command on the appropriate devices.

Solaris Clients

StoreOnce Catalyst over Fibre Channel presents a device type of **Processor**. On Solaris, the device files are created in `/dev/scsi/processor/*` location. After zoning the devices or changing the Number of Devices per Initiator Port, proceed as follows:

1. Scan for device file changes.
2. If you are a root user, execute the following commands:
   - `add_drv -vi scsiclass,03 sgen`
   - `update_drv -vai scsiclass,03 sgen`

   By default, `/dev/scsi/processor/*` devices are accessible only by the root users. For non-root user, provide the backup user permissions to access the device files using the `chmod -R o+rwx /dev/scsi/processor/*` command.
3. To get permissions for `/dev/scsi/processor/*` device files, use the Catalyst over Fibre Channel commands:

   ```
   for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep
   "Vendor|Product"; echo; done
   ```
4. Use the `chmod -R o+rwx` command on the appropriate devices.

Glossary

This glossary reflects terms relating to this document.

Term	Description
Backup to Disk (B2D) device	Disk-based backup device.
chunking (chunks)	The process of dividing data into blocks (chunks), where each chunk gets a unique content address. Internal storage unit of between 1.6 kB – 10 kB variable size (4 kB on average). Unique data chunks are stored in the deduplication store. A list of (references to) chunks makes up a portion.
D2D	Disk-to-disk storage. Generic name for disk-to-disk backups. For example, HPE StoreOnce Backup system offers D2D storage (and includes built-in deduplication).
deduplication	Process of eliminating duplicate data from an incoming data stream. Only unique data is written to the storage disk. During a restore operation, the original data stream is reconstructed (sometimes referred to as *rehydrated*).
deduplication daemon	See StoreOnceSoftware utility.
deduplication ratio (-rate)	Ratio between size of the source data to be backed up and the size of the actual data which is written to the store. For example, if 10 MB of source data results in only 1 MB of backed up data being written to store, the deduplication ration is 10:1.
deduplication store	See StoreOnce library.
deduplication system	Enables multiple Media Agents to work with the StoreOnce library simultaneously. Name of the *hosting* machine where the deduplication store is located (name of the server where the deduplication store is installed).
gateway	Gateways are clients with the Media Agent component installed. Sometimes referred to as a Media Agent host or gateway client. Each gateway represents a host on which multiple Media Agents can be started at the same time. Gateways are selected from a drop-down list of Data Protector clients that have the Media Agent component.
hardware deduplication	Deduplication is performed by the device to which data is backed up. See also target-side deduplication.
hash	A short fingerprint of a sequence of bytes, typically of a *chunk*. It uniquely identifies this chunk with a very high probability.
item	Externally addressable unit of storage in the deduplication store. It can represent Tape (for Virtual Tape personality), File (NFS) in the D2D appliance, and consists of *portions*. An item contains one or more object versions.
LUN	Logical unit number. A number which is used to identify a logical unit such as a device addressed by the SCSI protocol.
portion	Description of input data as list of hashes, variable size (10 MB on average), and limited by input data size or number of hashes. A portion is part of an Item. Portions do not overlap. The sequence of all portions of an item makes up the item.
server-side deduplication	Deduplication is done on the Media Agent system (gateway), so all the data needs to be transferred over the network between the Disk Agent and Media Agent (this is sometimes referred to as high-bandwidth transfer).
SHA-1	Cryptographic hash function. Secure hash algorithm.

source-side deduplication	Deduplication is done on the client machine, so only new, unique data needs to be transferred over the network (this is sometimes referred to as client-side deduplication or low-bandwidth transfer).
StoreOnce	All HPE StoreOnce products feature HPE StoreOnce deduplication software. Full product name: *HPE StoreOnce Backup system*.
StoreOnce library	Physical store used by StoreOnce software deduplication.
StoreOnceSoftware utility	The StoreOnceSoftware utility runs as a service (`StoreOnceSoftware.exe`) on Windows systems and as a background process (daemon) on Linux systems. A maintenance tool for performing general administration tasks on the deduplication store.
StoreOnce software deduplication	Interface type used by the Backup to Disk device. Provides software-based deduplication.
target-side deduplication	Deduplication is done on the target device, not by the Media Agent. This lowers the load on the backed up system but all the data needs to be transferred over the network between the Disk Agent and the target device (this is sometimes referred to as high-bandwidth transfer).
UPS	Uninterruptible power supply (or source). Battery backup when the mains electricity fails.

Index

For more information

Visit the following Data Protector online resources to get more information:

http://www.hp.com/go/dataprotector

http://www.hp.com/go/imhub/dataprotector

http://www.hp.com/go/d2d

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

4AA3-7696ENA, Created March 2016

Hewlett Packard
Enterprise