Setting up the DR Series system on HP® Data Protector 9.0

Technical White Paper

Quest Software Inc.

October 2017

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OFANY KIND

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Zmanda is a trademark of Zmanda Incorporated in the USA.All other trademarks and registered trademarks are property of their respective owners.

Legend

🟥 **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death**

❗ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Setting up the DR Series system on HP® Data Protector 9.0

Updated: December 22, 2017

Contents

Revisions

Date	Description
April 2015	Initial release
October 2017	Updated Quest-branded screen shots for the DR Series system release 4.0.3.

Executive Summary

This document provides information about how to set up the Quest DR Series system as a backup target for HP Data Protector 9.0

For additional documentation including other data management application (DMA) best practice whitepapers, see the system documentation for your specific DR Series system model at:

http://support.quest.com/DR-Series

> **NOTE:** The DR Series system/HP Data Protector build version and screenshots used for this document might vary slightly, depending on the version of the DR Series system/ HP Data Protector Software version you are using.

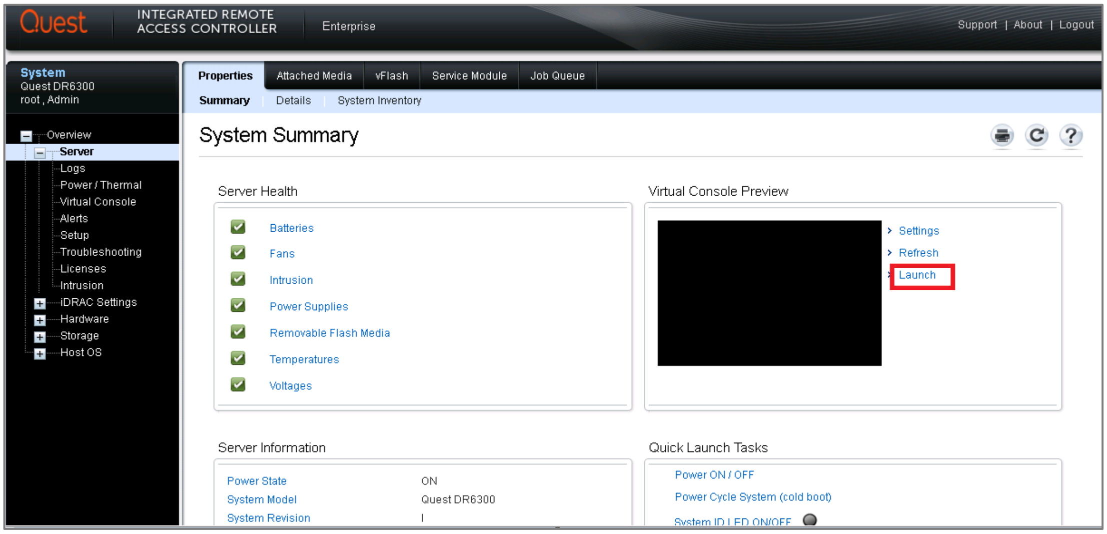
1

Installing and configuring the DR Series system

1 Rack and cable the DR Series system, and power it on. Refer to *Quest DR Series System Administrator Guide*, under sections of “iDRAC Connection”, “Logging in and Initializing the DR Series System”, and “Accessing IDRAC6/Idrac7 Using RACADM” for using iDRAC connection and initializing the appliance.

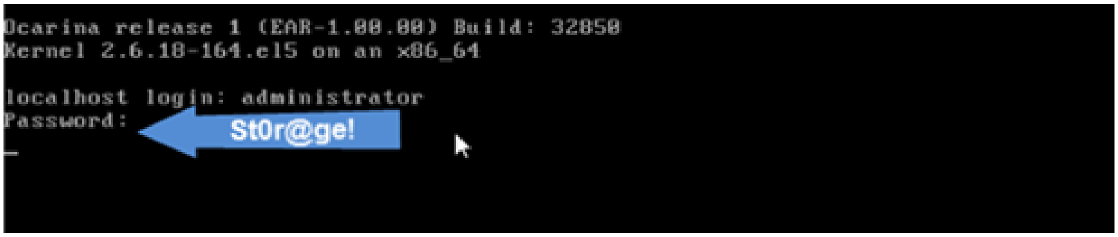
2 Log on to iDRAC using the default address 192.168.0.120 or the IP that is assigned to the iDRAC interface. Use the user name and password combination of “**root/calvin**”.

3 Launch the virtual console.



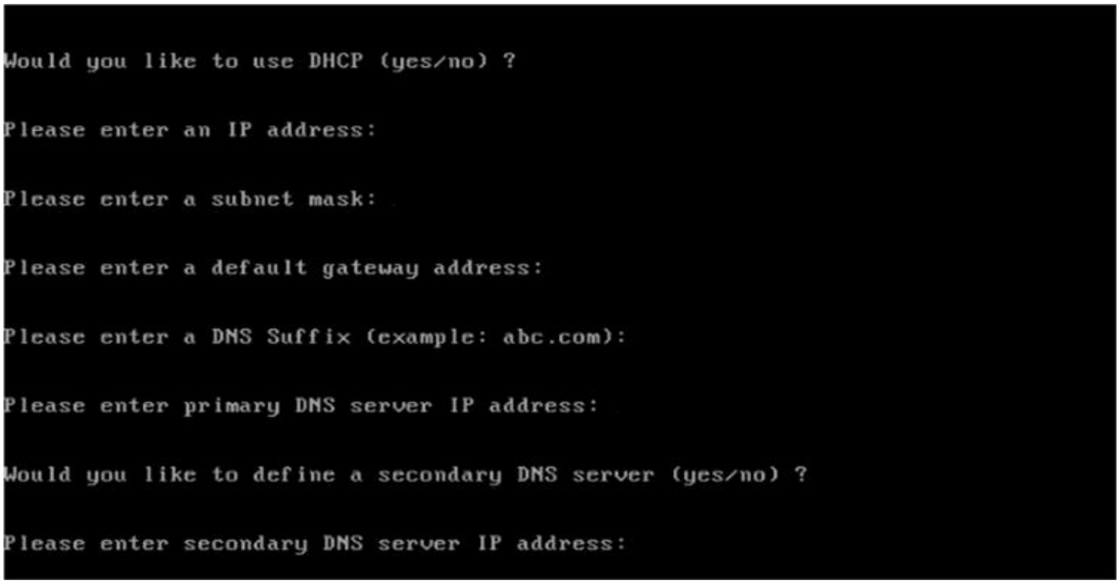
Power State ON
System Model Quest DR6300
System Revision I

4 After the virtual console is open, log on to the system as user **administrator** with the password **St0r@ge!** (The “0” in the password is the numeral zero).



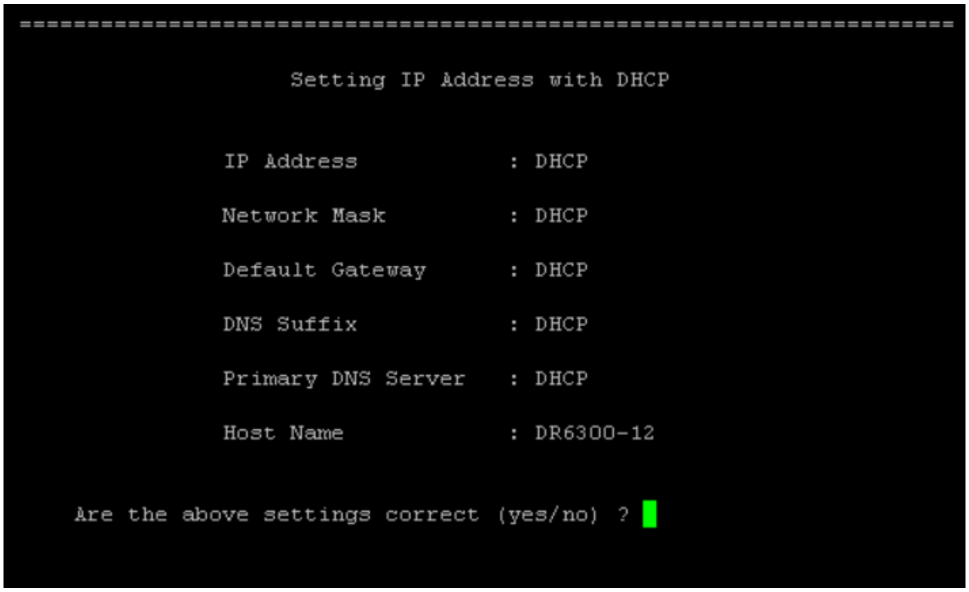
```
Ocarina release 1 (EAR-1.00.00) Build: 32850
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password:
_
```

5 Set the user-defined networking preferences.



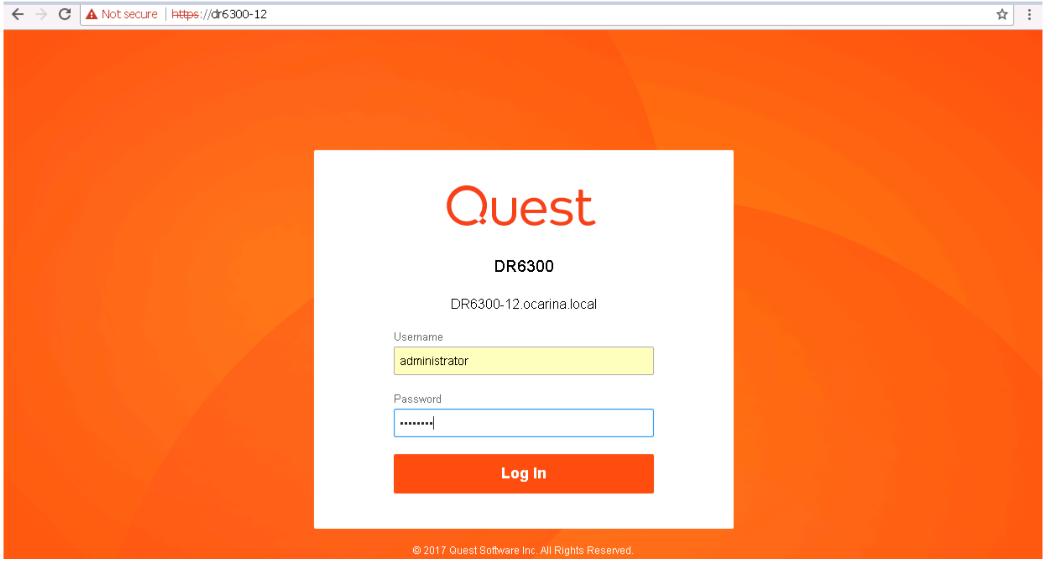
```
Would you like to use DHCP (yes/no) ?

Please enter an IP address:

Please enter a subnet mask:

Please enter a default gateway address:

Please enter a DNS Suffix (example: abc.com):

Please enter primary DNS server IP address:

Would you like to define a secondary DNS server (yes/no) ?

Please enter secondary DNS server IP address:
```

6 View the summary of preferences and confirm that it is correct.



```
======================================================================

                    Setting IP Address with DHCP

               IP Address             : DHCP

               Network Mask           : DHCP

               Default Gateway        : DHCP

               DNS Suffix             : DHCP

               Primary DNS Server     : DHCP

               Host Name              : DR6300-12

    Are the above settings correct (yes/no) ?
```

7 Log on to the DR Series system administrator console with the IP address with username **administrator** and password **St0r@ge!** (The “0” in the password is the numeral zero.).



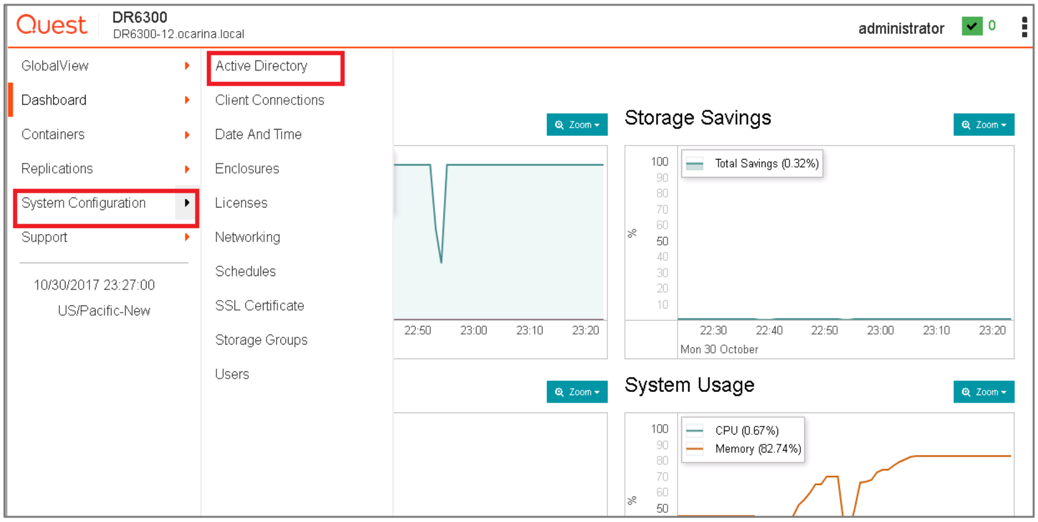
Username: administrator

Password: ••••••••

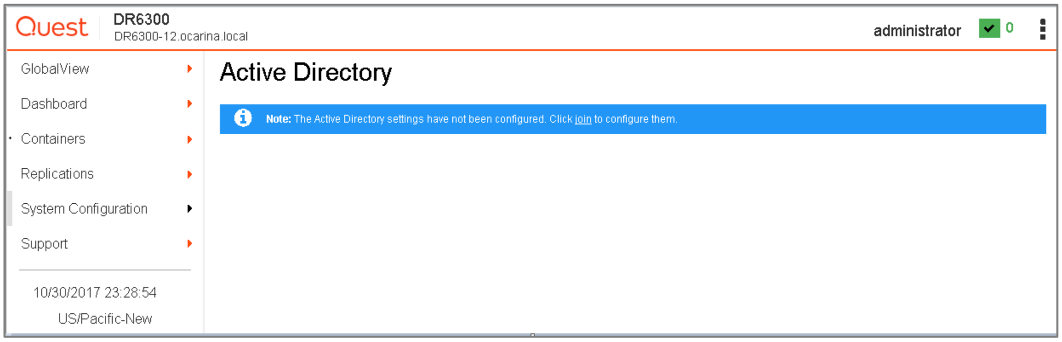
8 Join the DR Series System to Active Directory.

> **NOTE:** If you do not want to add DR Series system to Active Directory, see the *DR Series System Owner’s Manual* for guest logon instructions.

a Select **System Configuration** > **Active Directory** from the left navigation area of the DR Series system GUI.



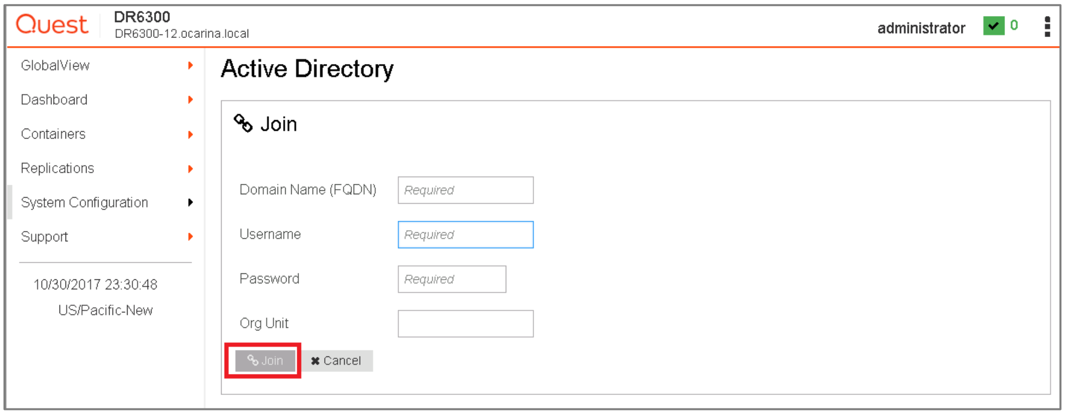
b Click the **Join** link.



Active Directory

Note: The Active Directory settings have not been configured. Click join to configure them.

c Enter your Active Directory credentials, and click **Join**.

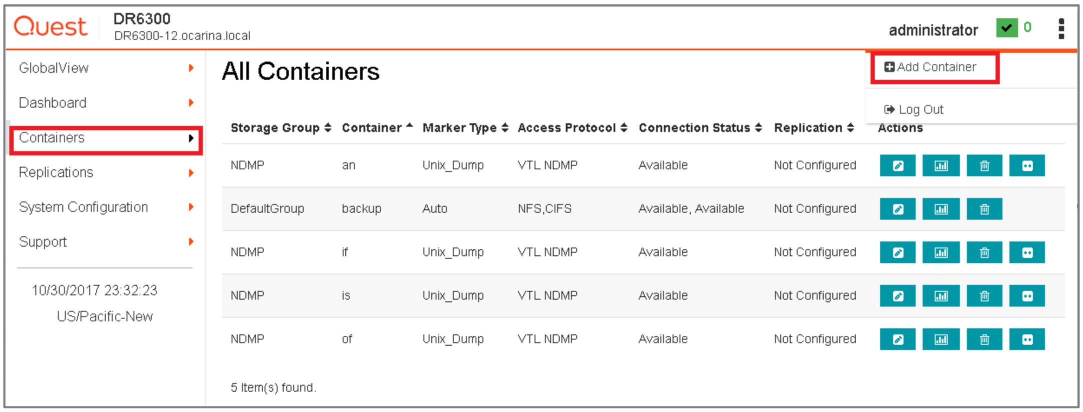


Active Directory

Join

Domain Name (FQDN)	Required
Username	Required
Password	Required
Org Unit	

9 Select **Containers** in the left navigation area of the DR Series system GUI, and then on the Action Menu in the upper right corner, click **Add Container**.

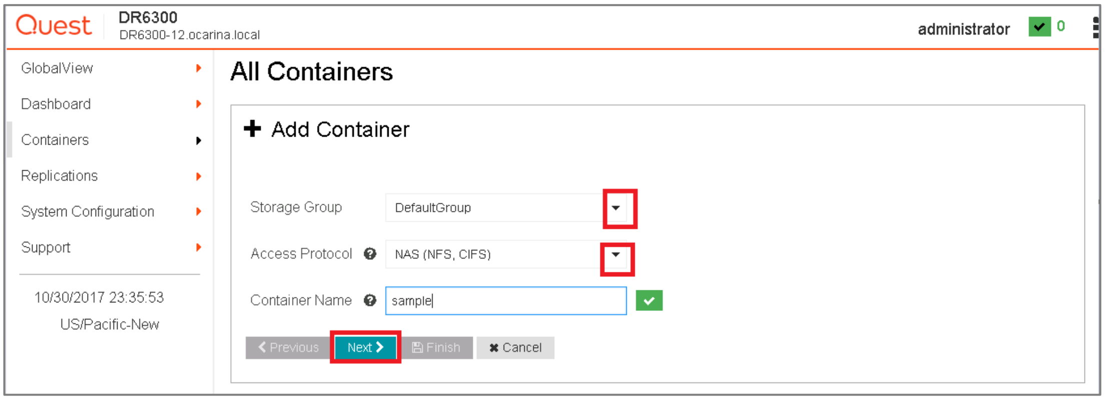


All Containers

Storage Group	Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
NDMP	an	Unix_Dump	VTL NDMP	Available	Not Configured	
DefaultGroup	backup	Auto	NFS,CIFS	Available, Available	Not Configured	
NDMP	if	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	is	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	of	Unix_Dump	VTL NDMP	Available	Not Configured	

5 Item(s) found.

10 Select the required Storage group, enter a **Container Name**, select the **NAS (NFS, CIFS)** from the Access Protocol drop down menu, and click **Next**



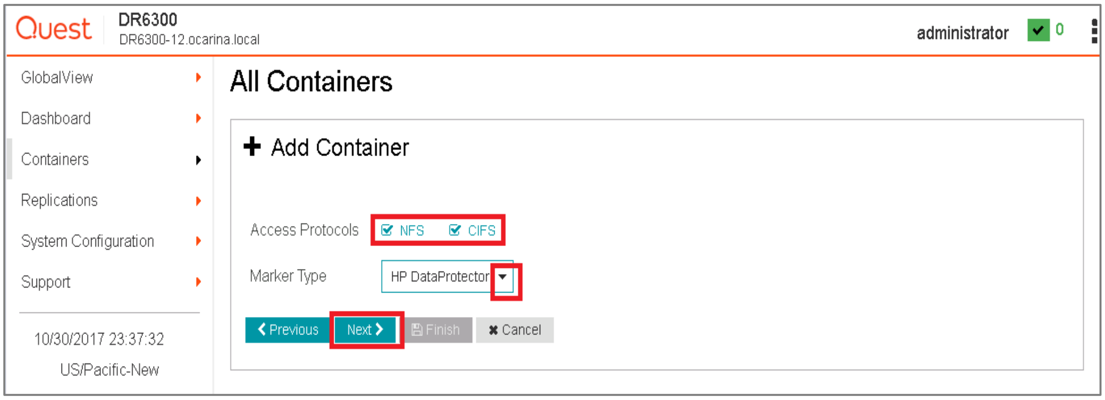
Storage Group: DefaultGroup

Access Protocol: NAS (NFS, CIFS)

Container Name: sample

11 Select the protocols NFS and/or CIFS as required, select the Marker type as **HP Data Protector** from the drop down menu, and click **Next**.

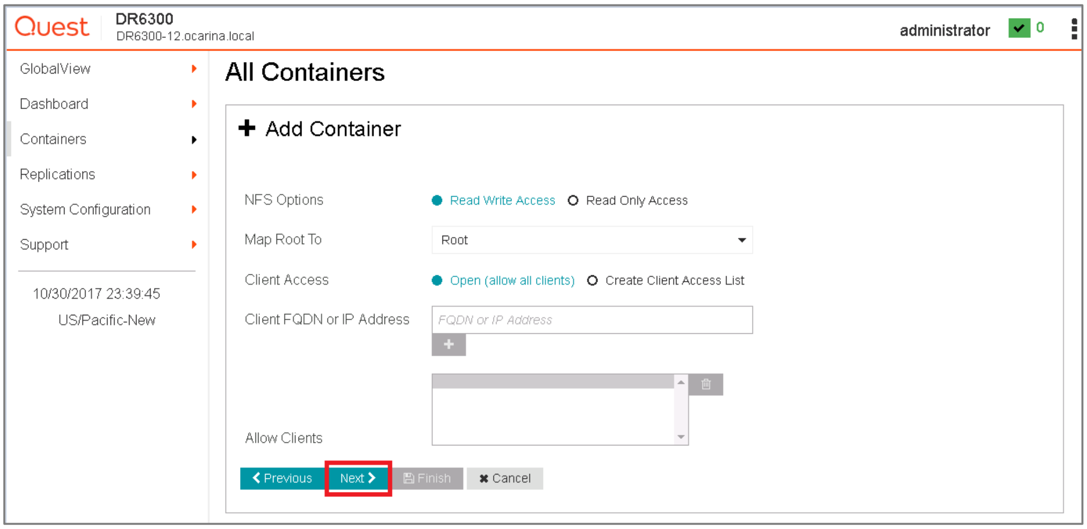
NOTE: HP Data Protector supports both the CIFS and NFS protocols.



Access Protocols: ☑ NFS ☑ CIFS

Marker Type: HP DataProtector

12 For NFS, select the preferred client access credentials and click **Next**.



NFS Options: ● Read Write Access ○ Read Only Access

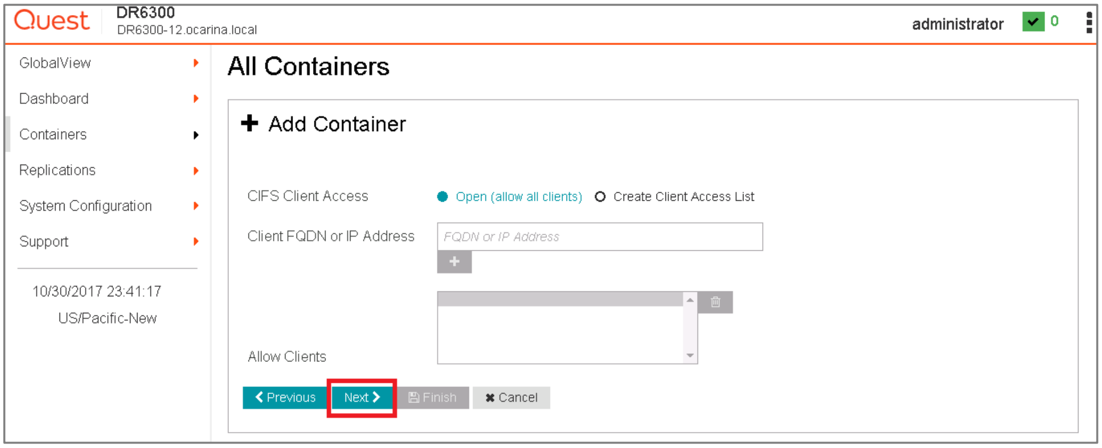
Map Root To: Root

Client Access: ● Open (allow all clients) ○ Create Client Access List

Client FQDN or IP Address: FQDN or IP Address

Allow Clients

13 For CIFS, select the Client Access credentials and click **Next**.

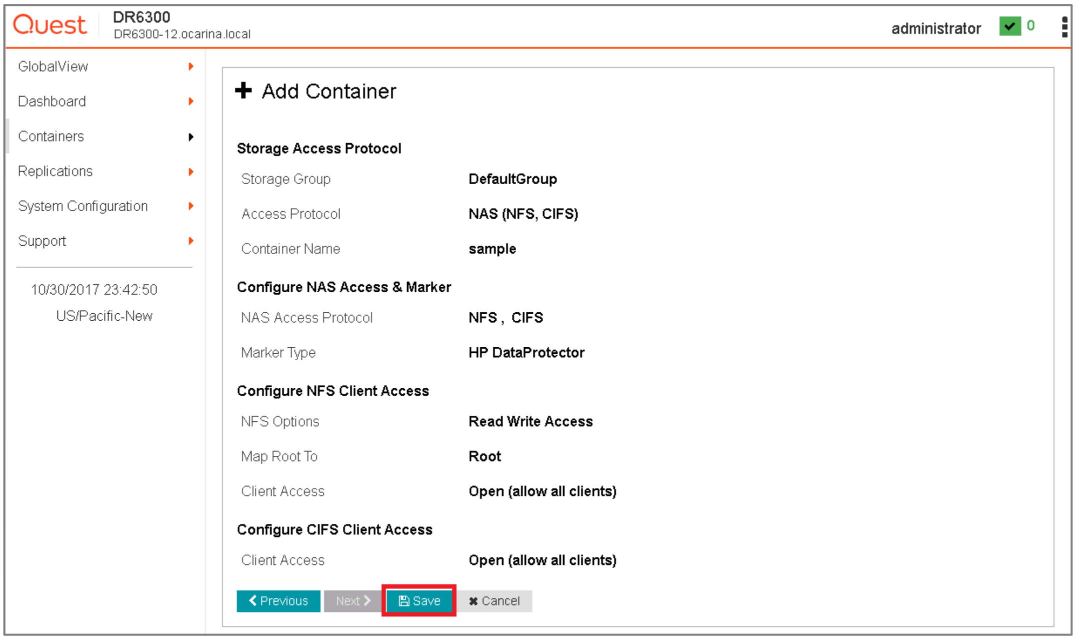


CIFS Client Access: ● Open (allow all clients) ○ Create Client Access List

Client FQDN or IP Address

NOTE: For improved security, Quest recommends adding IP addresses for the following (Not all environments will have all components): Backup console (HP Data Protector Server, HP Data Protector Clients)

14 Check the configuration summary and click **Save**.



Storage Access Protocol

Storage Group	**DefaultGroup**
Access Protocol	**NAS (NFS, CIFS)**
Container Name	**sample**

Configure NAS Access & Marker

NAS Access Protocol	**NFS , CIFS**
Marker Type	**HP DataProtector**

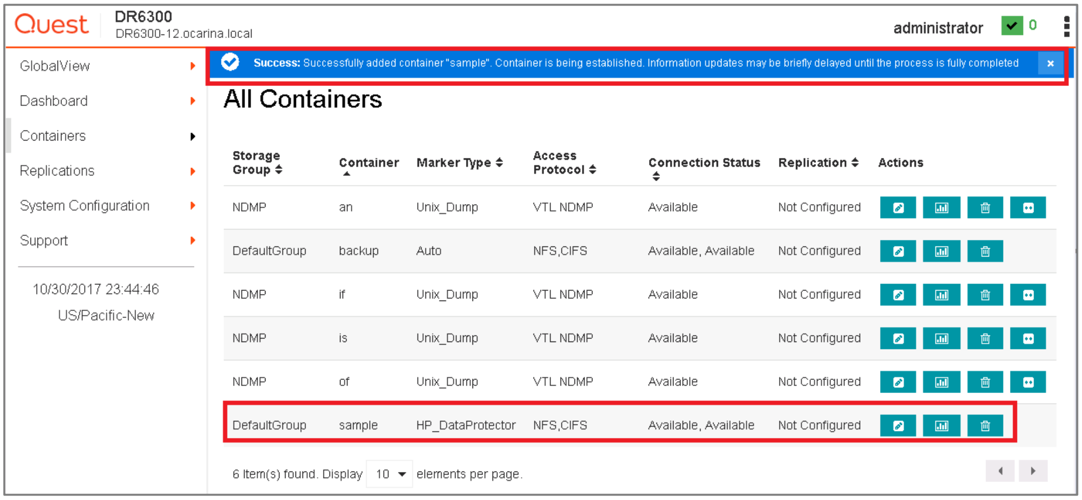
Configure NFS Client Access

NFS Options	**Read Write Access**
Map Root To	**Root**
Client Access	**Open (allow all clients)**

Configure CIFS Client Access

Client Access	**Open (allow all clients)**

15 Confirm the container is successfully created.



Success: Successfully added container "sample". Container is being established. Information updates may be briefly delayed until the process is fully completed

All Containers

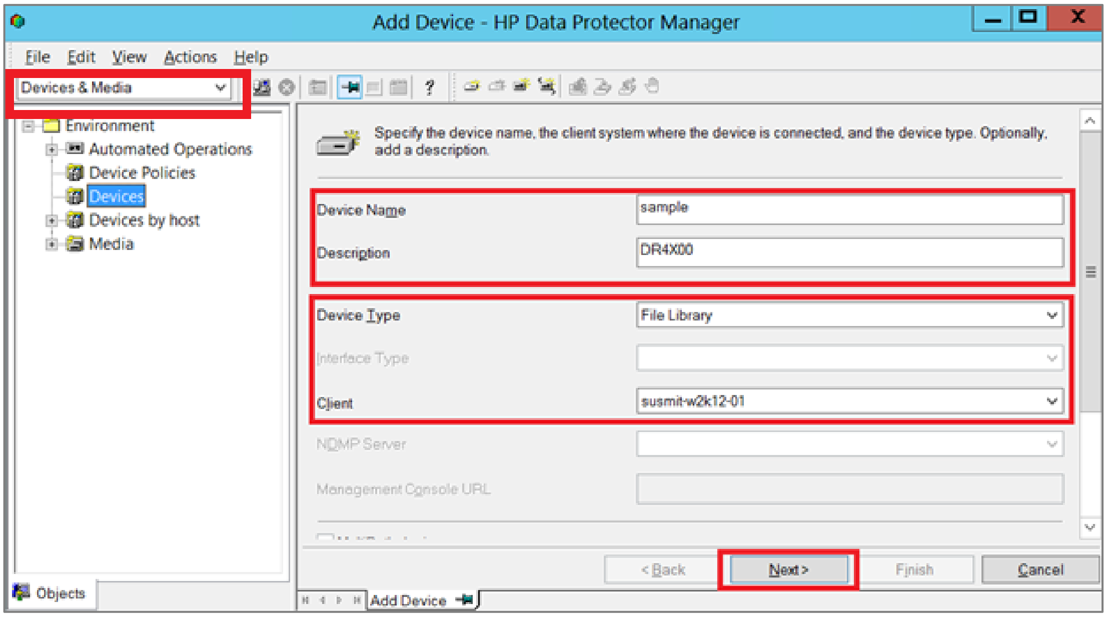
Storage Group	Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
NDMP	an	Unix_Dump	VTL NDMP	Available	Not Configured	
DefaultGroup	backup	Auto	NFS,CIFS	Available, Available	Not Configured	
NDMP	if	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	is	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	of	Unix_Dump	VTL NDMP	Available	Not Configured	
DefaultGroup	sample	HP_DataProtector	NFS,CIFS	Available, Available	Not Configured	

6 Item(s) found. Display 10 elements per page.

Setting up HP Data Protector

Backing up in the Windows environment

1. Open **HP Data Protector Manager** and select **Devices & Media** menu.
2. Right-click **Devices** and choose **Add Device**.
3. In the next window, specify the **Device Name** and **Description** that identifies the **File Library Device**.
4. Select **File Library** for the **Device Type**, select the required **Client**, and click **Next**.



Specify the device name, the client system where the device is connected, and the device type. Optionally, add a description.

Device Name: sample

Description: DR4X00

Device Type: File Library

Interface Type:

Client: susmit-w2k12-01

NDMP Server:

Management Console URL:

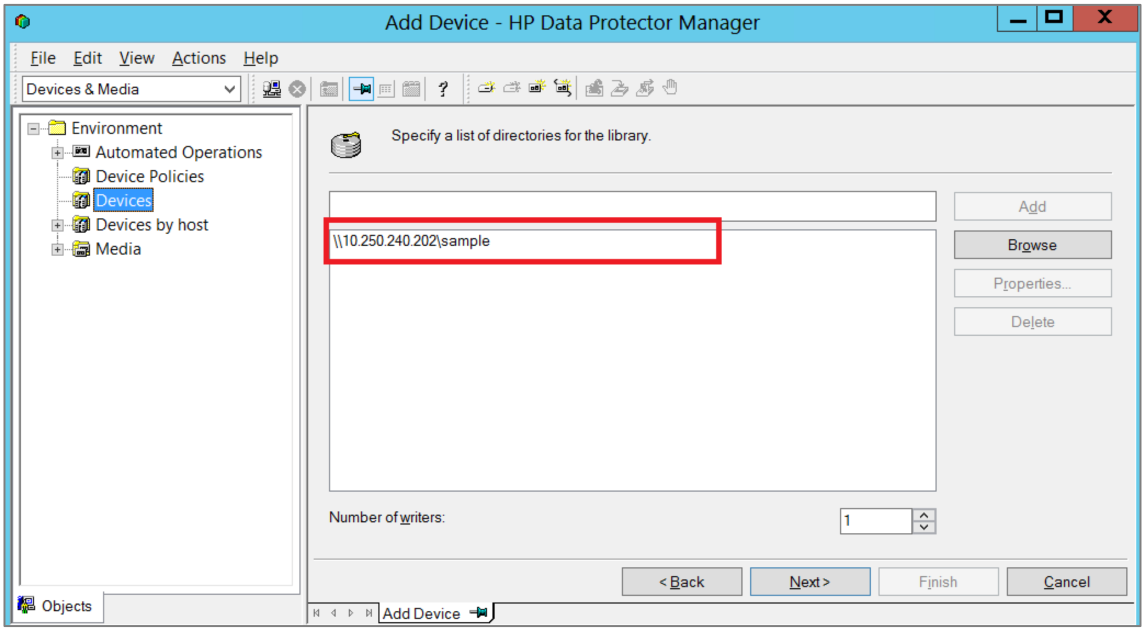
> NOTE: The Windows service account for HP Data Protector requires appropriate permissions to the DR container share for the step below to complete successfully. See **Appendix A** for setting up the HP Data Protector service account correctly. This should be done before the next step.

5 In the next window, enter the path to the library, which will be the UNC path to the DR Series container share as described below.

a Specify a list of directories for the library. You can also specify the **number of writers** for the library, it defaults to 1.

b Click **Properties** to assign proper values to the file library parameters, including Maximal File Size.

c Click **Next**.



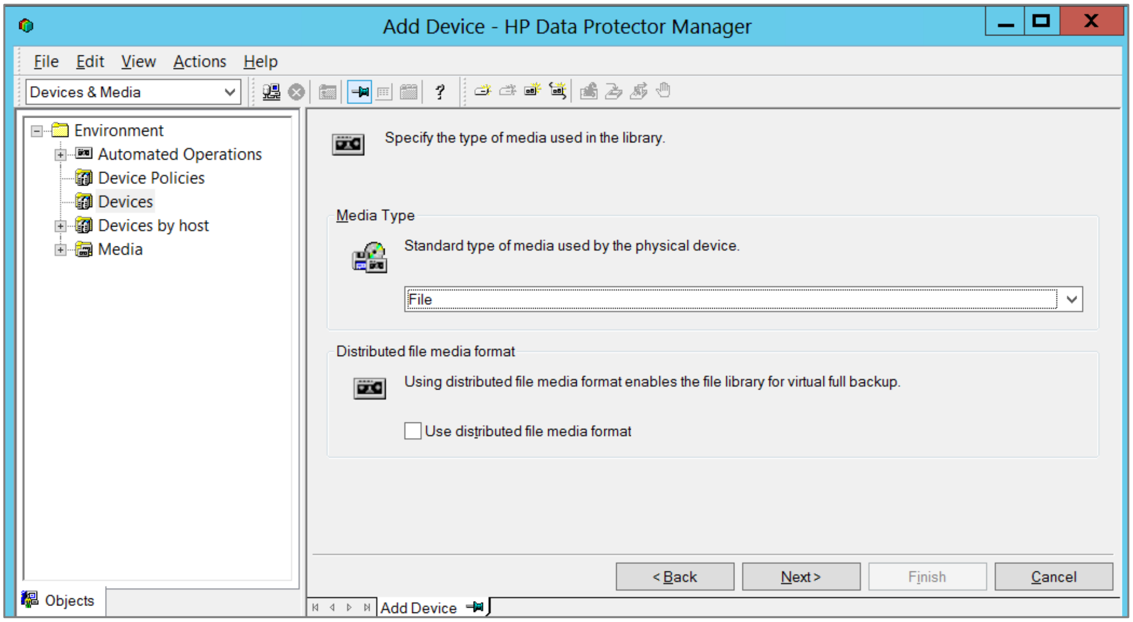
Add Device - HP Data Protector Manager

Specify a list of directories for the library.

\\10.250.240.202\sample

Number of writers: 1

6 Verify the **Media Type** default is **File**, and click **Next**.



Specify the type of media used in the library.

Media Type

Standard type of media used by the physical device.

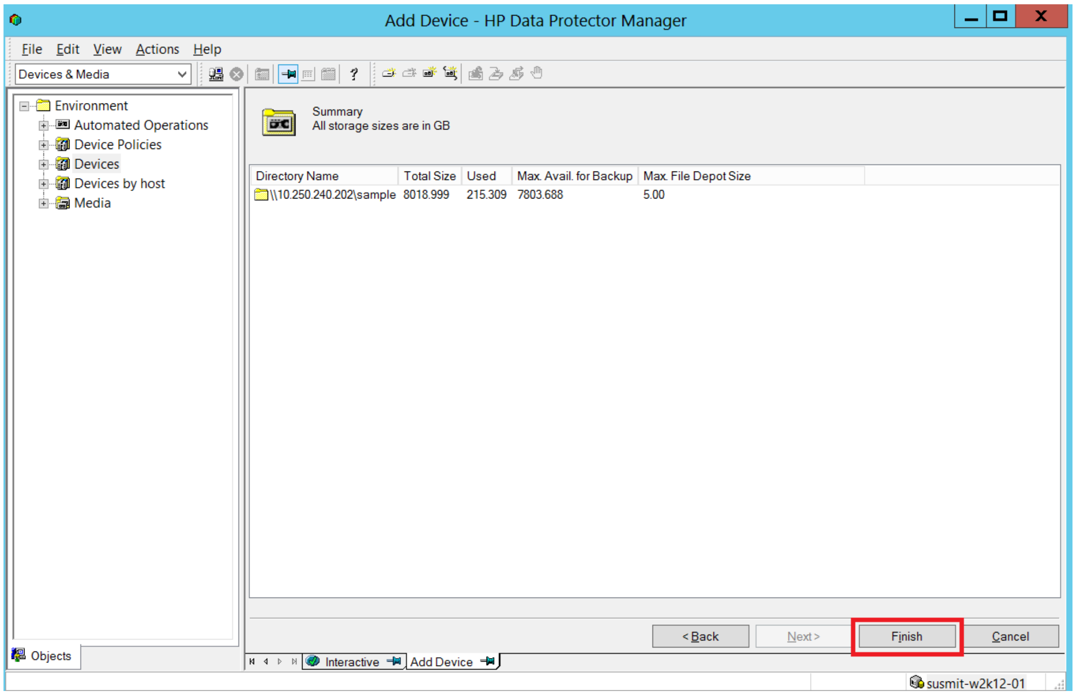
File

Distributed file media format

Using distributed file media format enables the file library for virtual full backup.

□ Use distributed file media format

7 In the **Summary** window, verify that it shows the total physical storage size of that particular File Library Device on the DR container, and click **Finish**.



Summary
All storage sizes are in GB

Directory Name	Total Size	Used	Max. Avail. for Backup	Max. File Depot Size
\\10.250.240.202\sample	8018.999	215.309	7803.688	5.00

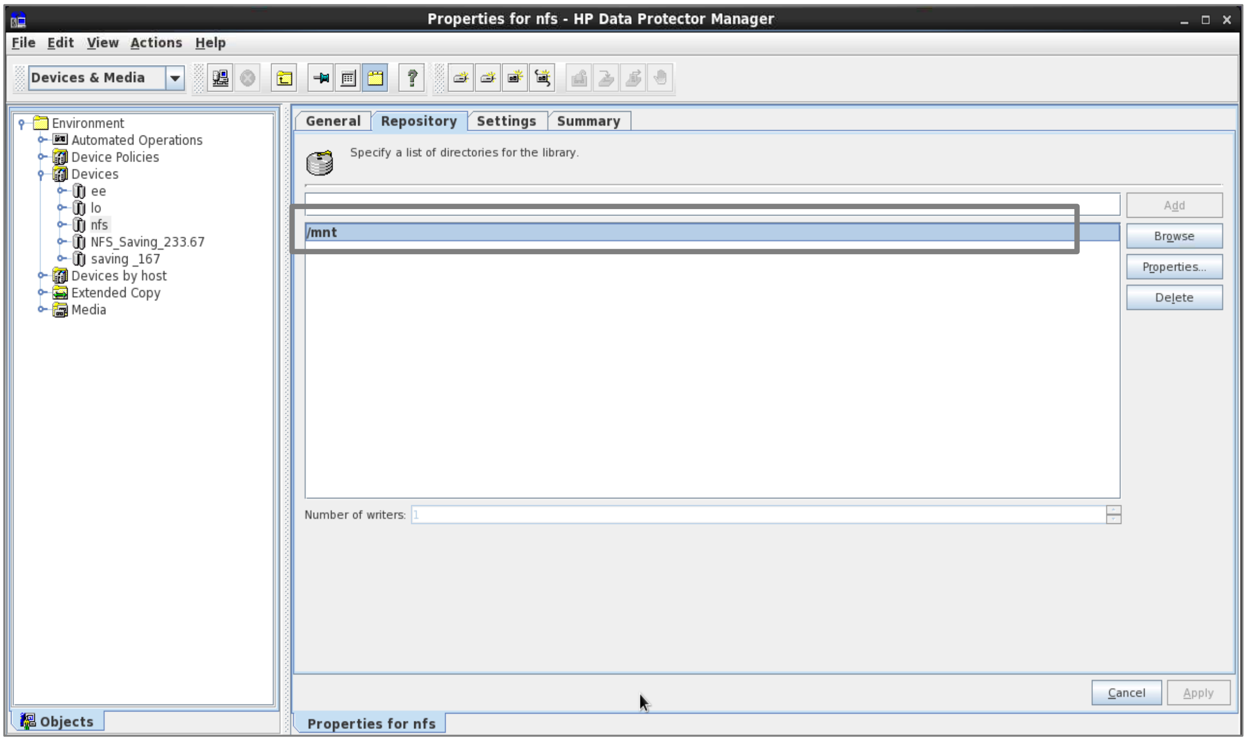
8 In the next windows, click **Close**.

Backing up in the Unix/Linux environment

NOTE: Make sure that you can mount/verify the NFS share from the UNIX/Linux client system. See **Appendix B** for information on how to mount/verify the NFS share.

The procedure for the Unix/Linux Environment is very similar to the procedure for the Windows environment. One difference is that in **Step#3**, you need to enter the UNIX path of the DR container export is used instead of a UNC path, as described below.

For other details, please refer to the preceding steps for backing up in the Windows environment.



Specify a list of directories for the library.

/mnt

Number of writers: 1

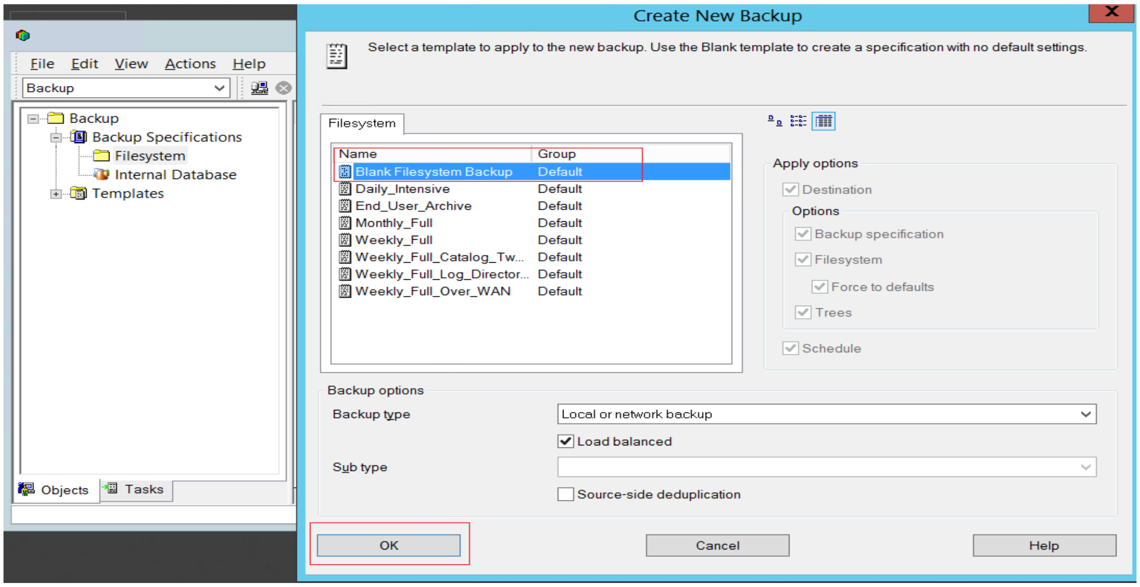
Creating a new backup job with the DR Series system as the target

1 In the **Context List** drop-down menu, click **Backup**.

2 In the **Scoping Pane**, expand **Backup** and then click **Backup Specifications**.

3 In the expanded sub-tree view, right-click the **Filesystem** item and select **Add Backup**.

4 Select the **Blank File System Backup** template and click **OK**.



Create New Backup

Select a template to apply to the new backup. Use the Blank template to create a specification with no default settings.

Name	Group
Blank Filesystem Backup	Default
Daily_Intensive	Default
End_User_Archive	Default
Monthly_Full	Default
Weekly_Full	Default
Weekly_Full_Catalog_Tw...	Default
Weekly_Full_Log_Director...	Default
Weekly_Full_Over_WAN	Default

Apply options

☑ Destination

Options

☑ Backup specification

☑ Filesystem

☑ Force to defaults

☑ Trees

☑ Schedule

Backup options

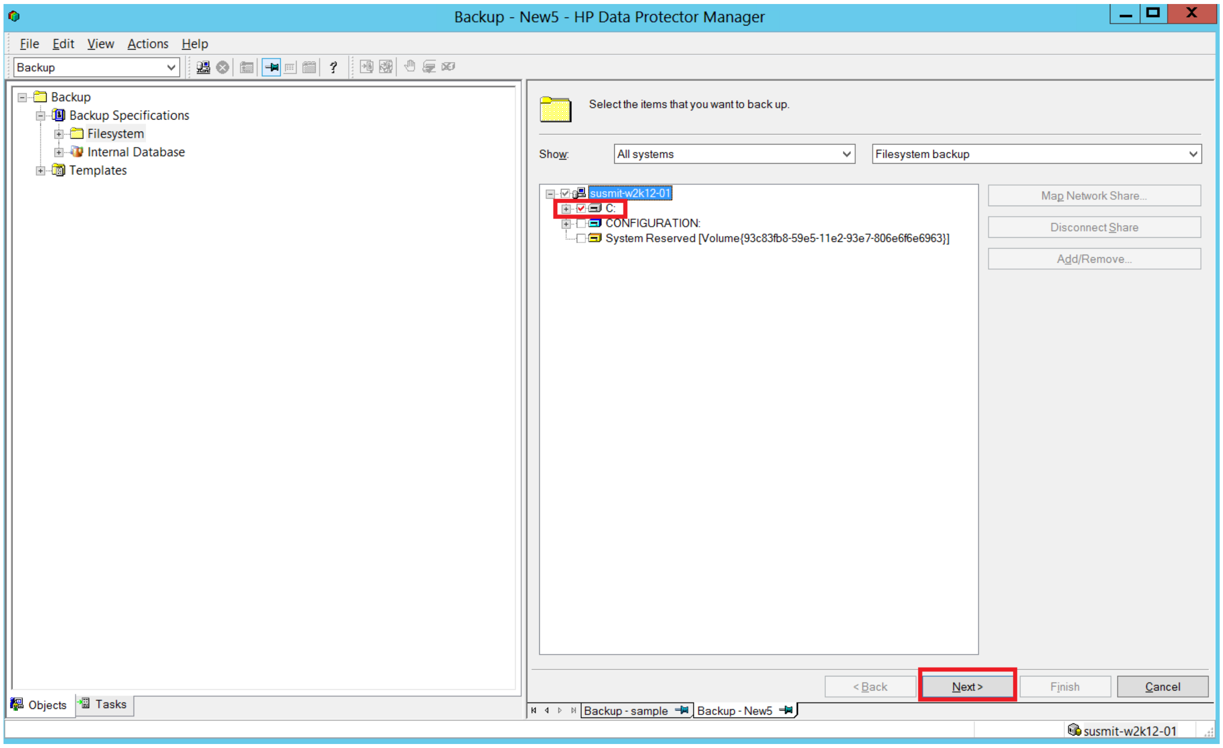
Backup type: Local or network backup

☑ Load balanced

Sub type:

☐ Source-side deduplication

5 Check any source data set that needs to be backed up, (in this example, the entire local “C:\” drive is selected) and then click **Next**.

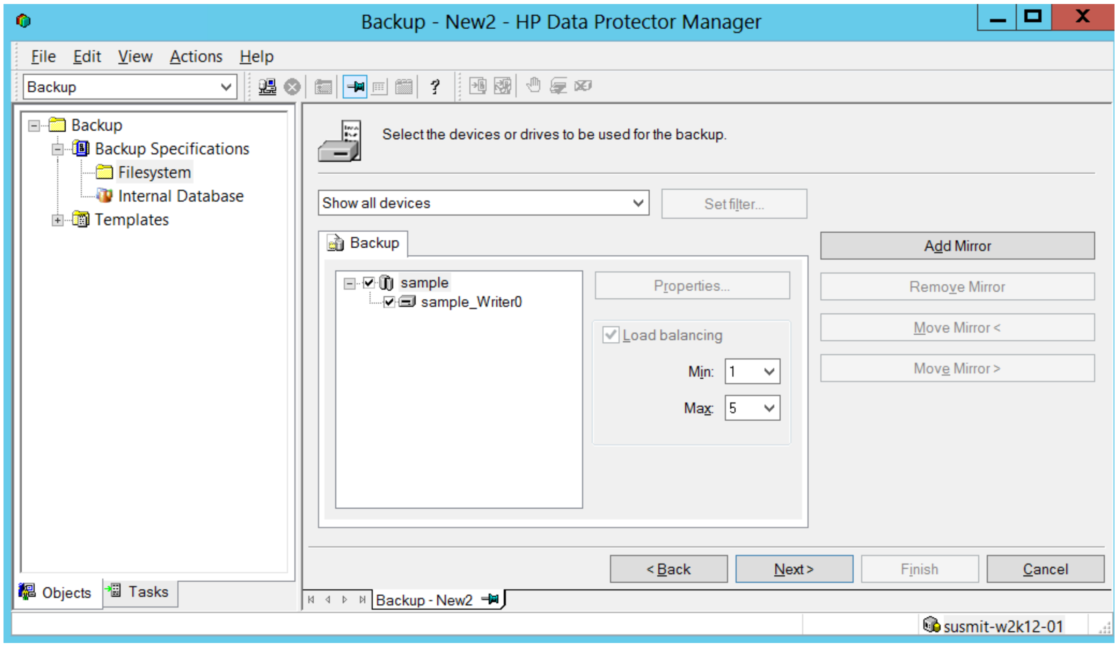


Select the items that you want to back up.

Show: All systems | Filesystem backup

- ☑ susmit-w2k12-01
  - ☑ C:
  - □ CONFIGURATION:
  - □ System Reserved [Volume{93c83fb8-59e5-11e2-93e7-806e6f6e6963}]

6 Select the devices or drives to be used as the backup target (in this example, it is the DR Series container share/export created in the previous section), and click **Next**.



Select the devices or drives to be used for the backup.

Show all devices

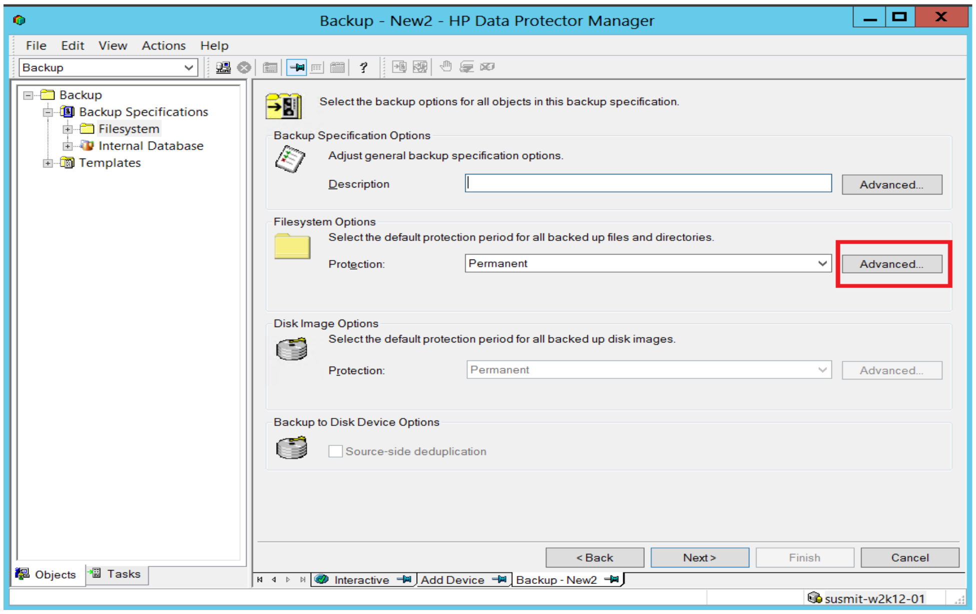
- ☑ sample
  - ☑ sample_Writer0

☑ Load balancing

Min: 1

Max: 5

7 Check and verify the **Backup Specification** Options through the **Advanced** button. Then in **Filesystem Options** section, click on **Advanced**.



Select the backup options for all objects in this backup specification.

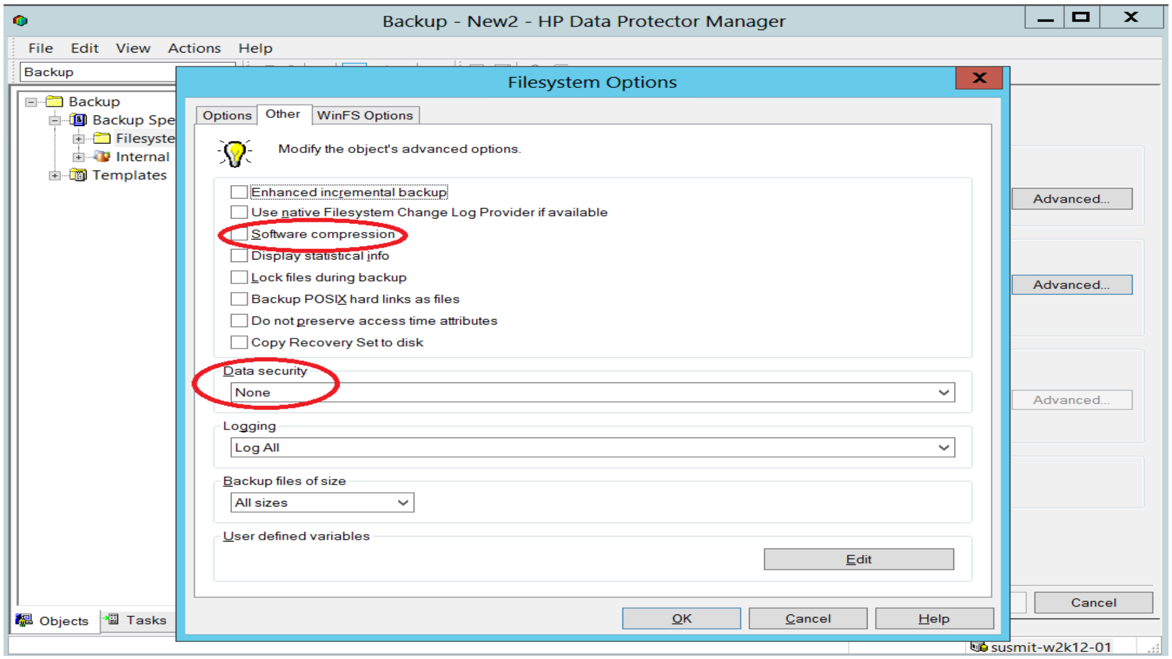
Backup Specification Options
Adjust general backup specification options.
Description: (blank) [Advanced...]

Filesystem Options
Select the default protection period for all backed up files and directories.
Protection: Permanent [Advanced...]

Disk Image Options
Select the default protection period for all backed up disk images.
Protection: Permanent [Advanced...]

Backup to Disk Device Options
□ Source-side deduplication

8 In **Filesystem Options**, click the **Other** tab, make sure **Software compression**” is not selected, and that **Data security** is set to **None**.



Modify the object's advanced options.

□ Enhanced incremental backup
□ Use native Filesystem Change Log Provider if available
□ Software compression
□ Display statistical info
□ Lock files during backup
□ Backup POSIX hard links as files
□ Do not preserve access time attributes
□ Copy Recovery Set to disk

Data security: None

Logging: Log All

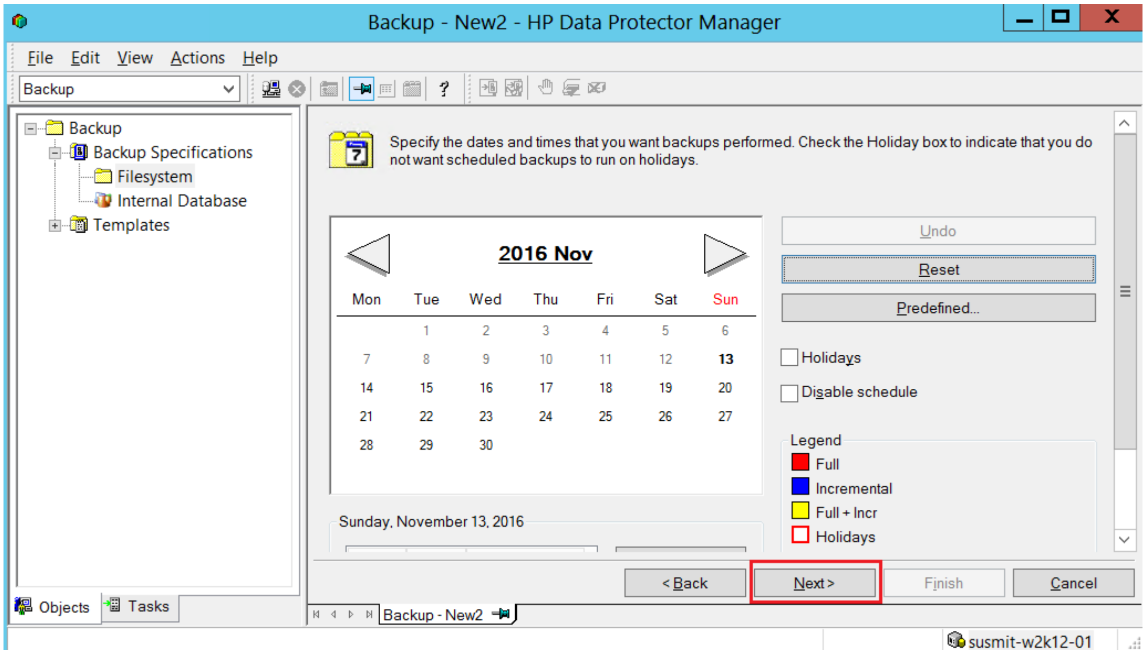
Backup files of size: All sizes

User defined variables [Edit]

NOTE: Always disable **'Software compression'**, as the DR Series system has compression built-in and does not require compression on HP Data Protector. In general, additional data compression on backup software can have a negative impact on total savings in the DR Series System.

Set **Data security** to **none**, as enabling encryption before the data stream is sent to the DR Series System device will make the data unable to be deduplicated. This can put a significant negative impact on the total savings of the DR Series system.

9 Define the Backup Job Schedule options and click **Next**.



Specify the dates and times that you want backups performed. Check the Holiday box to indicate that you do not want scheduled backups to run on holidays.

2016 Nov

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Sunday, November 13, 2016

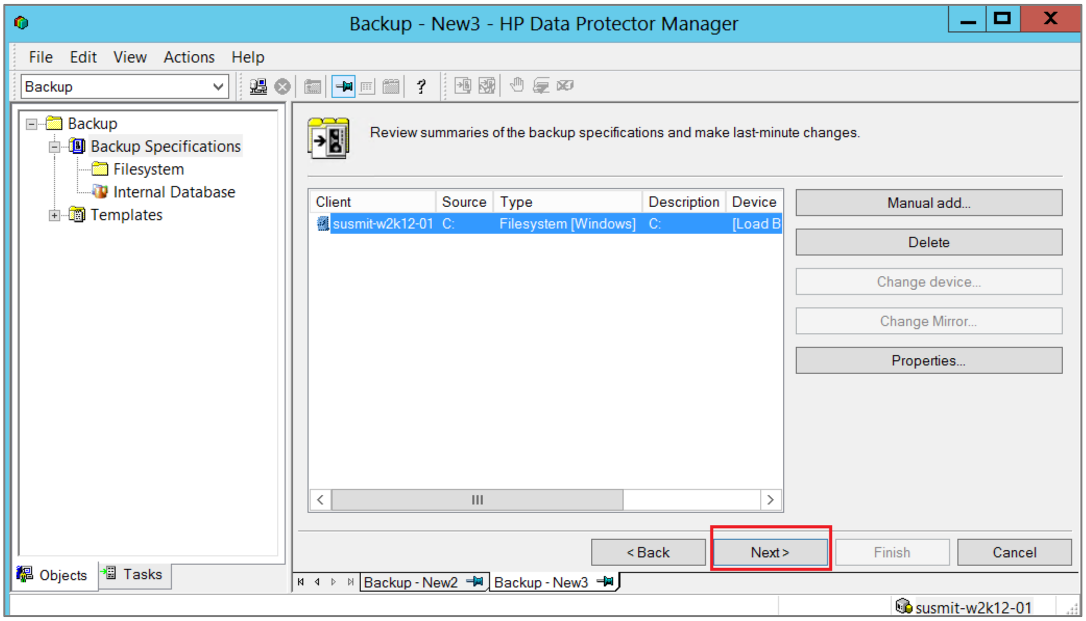
☐ Holidays

☐ Disable schedule

Legend

- 🟥 Full
- 🟦 Incremental
- 🟨 Full + Incr
- □ Holidays

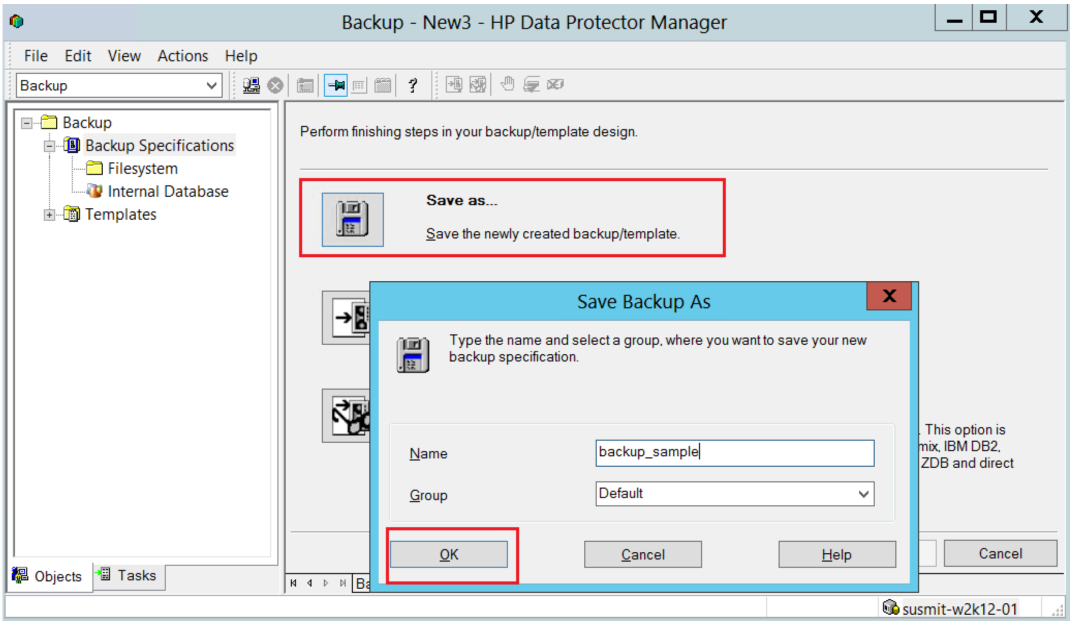
10 Review the Backup Job Summary, and click **Next**.



Review summaries of the backup specifications and make last-minute changes.

Client	Source	Type	Description	Device
susmit-w2k12-01	C:	Filesystem [Windows]	C:	[Load B

11 Specify a name for the Backup Job, and click **Save As** to save the newly configured backup specification.



Perform finishing steps in your backup/template design.

Save as...

Save the newly created backup/template.

Save Backup As

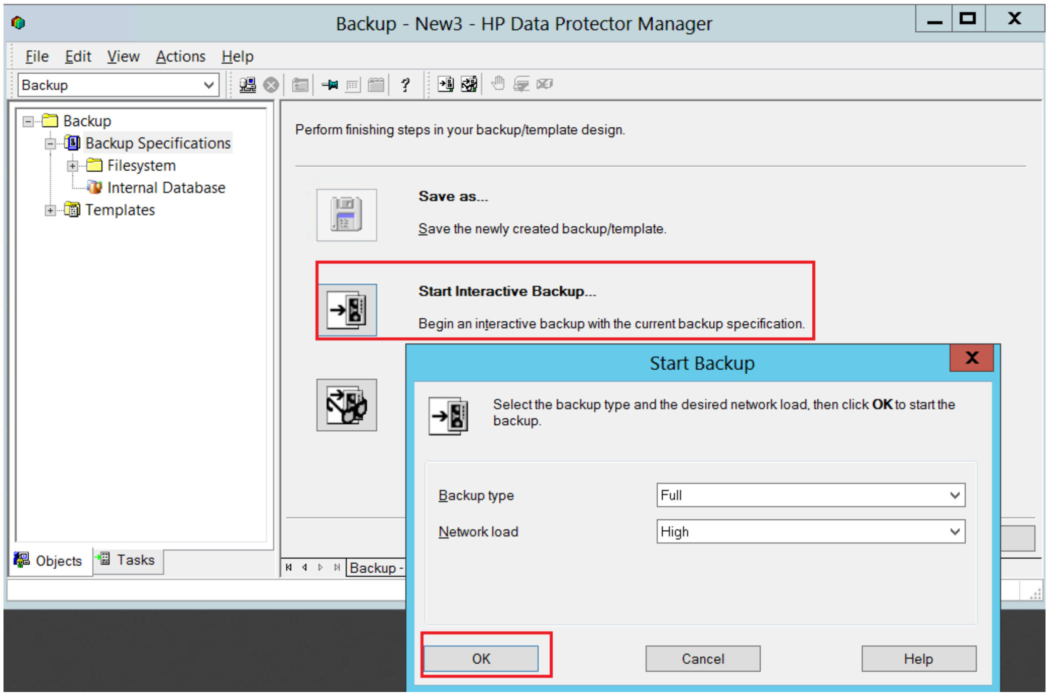
Type the name and select a group, where you want to save your new backup specification.

Name: backup_sample

Group: Default

OK | Cancel | Help

12 (**Optional**) Click **Start Interactive Backup** to run the backup, and, when the **Start Backup** window opens, click **OK** to start the backup.



Perform finishing steps in your backup/template design.

Save as...

Save the newly created backup/template.

Start Interactive Backup...

Begin an interactive backup with the current backup specification.

Start Backup

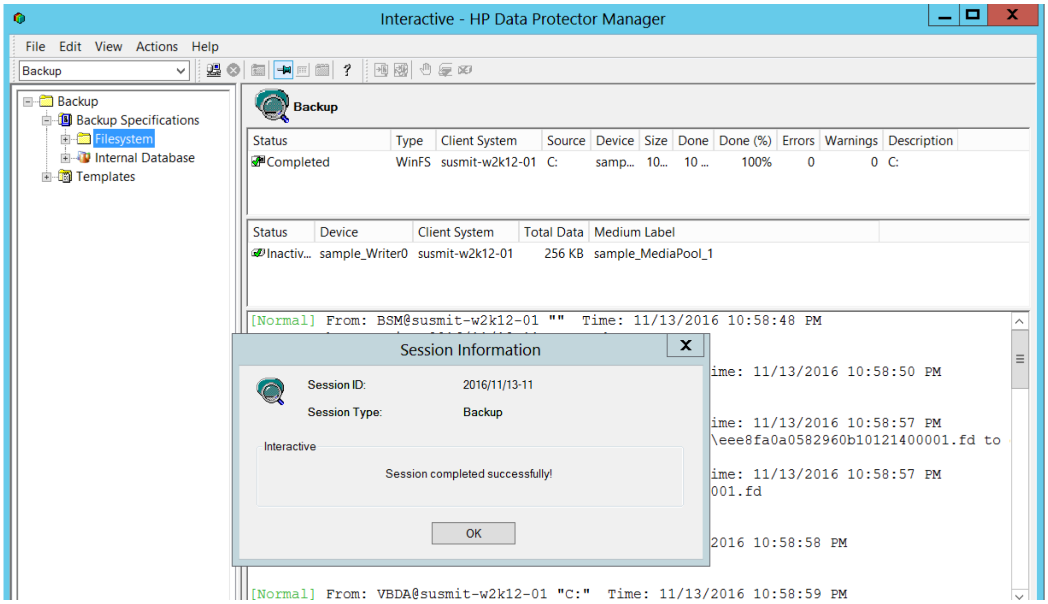
Select the backup type and the desired network load, then click **OK** to start the backup.

Backup type: Full

Network load: High

OK | Cancel | Help

The **Backup** window displays the progress of the backup session. The Session Information window will tell you when the backup is completed.



Status	Type	Client System	Source	Device	Size	Done	Done (%)	Errors	Warnings	Description
Completed	WinFS	susmit-w2k12-01	C:	samp...	10...	10 ...	100%	0	0	C:

Status	Device	Client System	Total Data	Medium Label
Inactiv...	sample_Writer0	susmit-w2k12-01	256 KB	sample_MediaPool_1

```
[Normal] From: BSM@susmit-w2k12-01 ""  Time: 11/13/2016 10:58:48 PM

ime: 11/13/2016 10:58:50 PM

ime: 11/13/2016 10:58:57 PM
\eee8fa0a0582960b10121400001.fd to

ime: 11/13/2016 10:58:57 PM
001.fd

2016 10:58:58 PM

[Normal] From: VBDA@susmit-w2k12-01 "C:"  Time: 11/13/2016 10:58:59 PM
```

Session Information

Session ID: 2016/11/13-11

Session Type: Backup

Interactive

Session completed successfully!

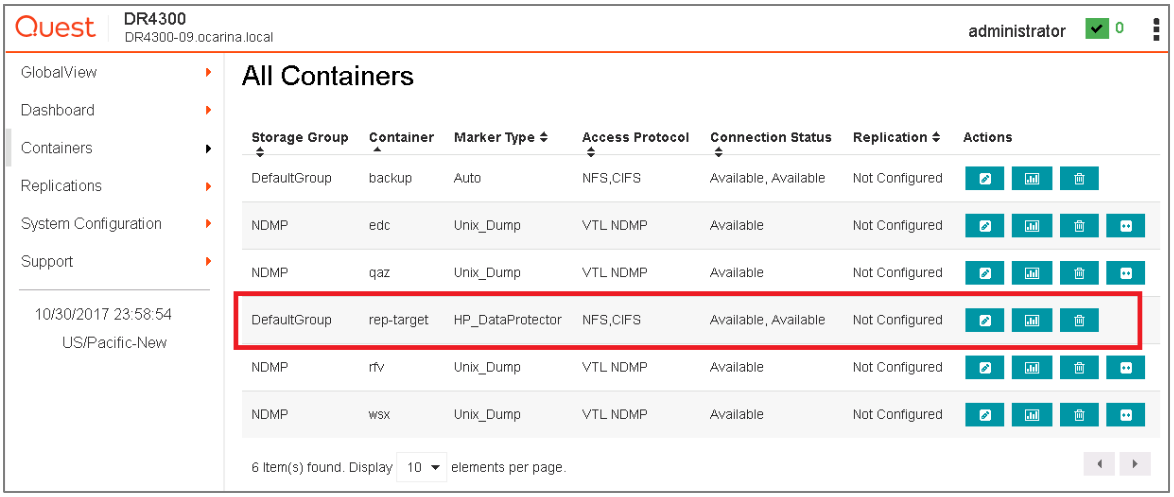
4

Setting up DR Series native replication and restoring from a target container

Building a replication relationship between DR Series systems

> **NOTE:** The assumption is that on both the source and target DR, a container is already created for each of them. The target container should not be used by anything else and is empty, with the same **Connection Type** as the source container.

1 Create a target container on the target DR Series system.

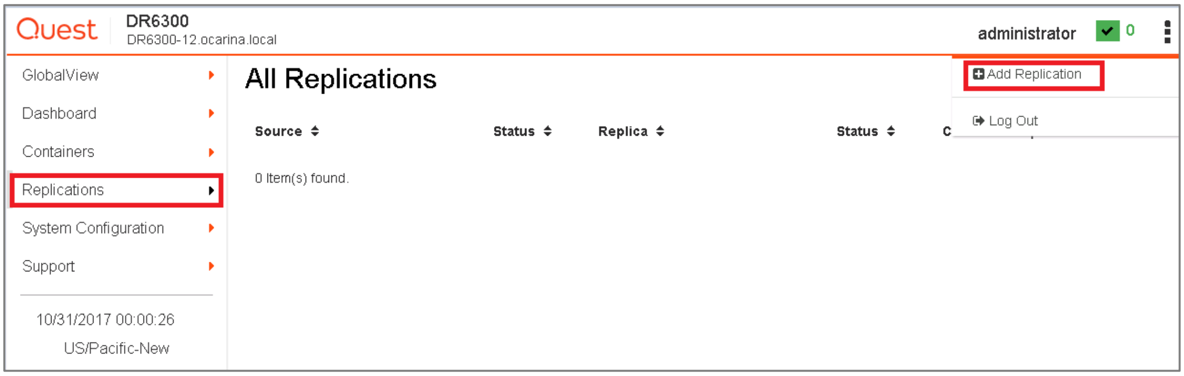


All Containers

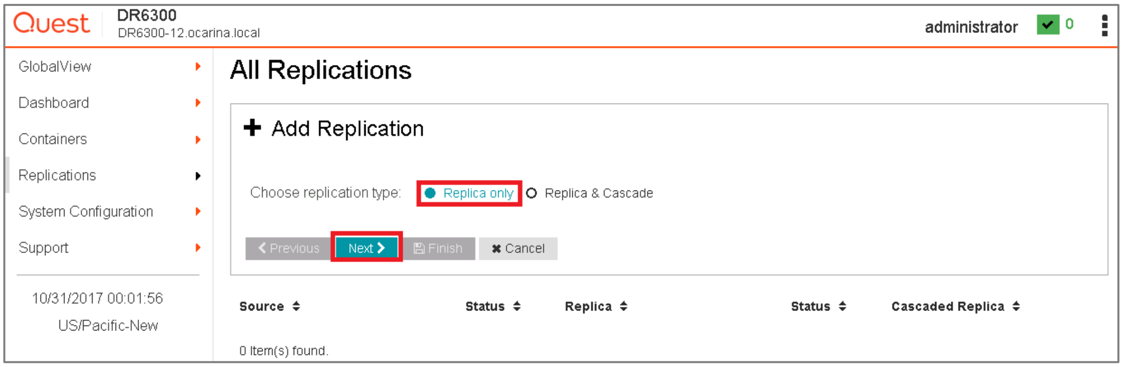
Storage Group	Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
DefaultGroup	backup	Auto	NFS,CIFS	Available, Available	Not Configured	
NDMP	edc	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	qaz	Unix_Dump	VTL NDMP	Available	Not Configured	
DefaultGroup	rep-target	HP_DataProtector	NFS,CIFS	Available, Available	Not Configured	
NDMP	rfv	Unix_Dump	VTL NDMP	Available	Not Configured	
NDMP	wsx	Unix_Dump	VTL NDMP	Available	Not Configured	

6 Item(s) found. Display 10 elements per page.

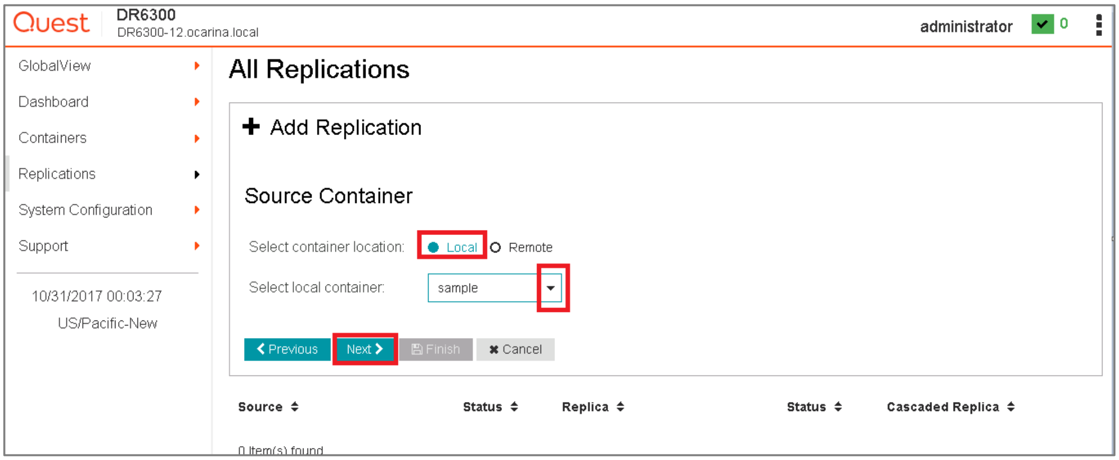
2 On the source DR Series system, select **Replications** from the left navigation menu, and, on the Actions menu, click **Add Replication**.



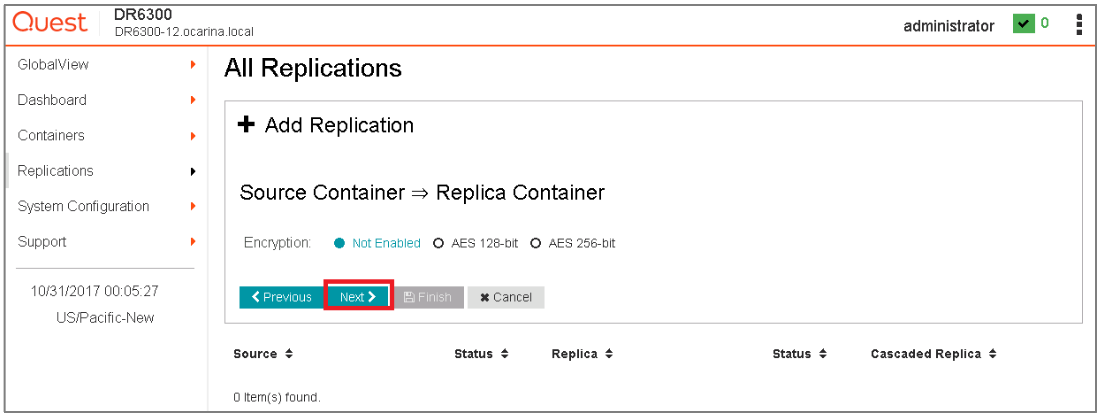
3 Select the type of Replication and click **Next.**



4 Select the source container to be replicated, and click '**Next**'



5 Select an encryption mode if required, and click **Next**.

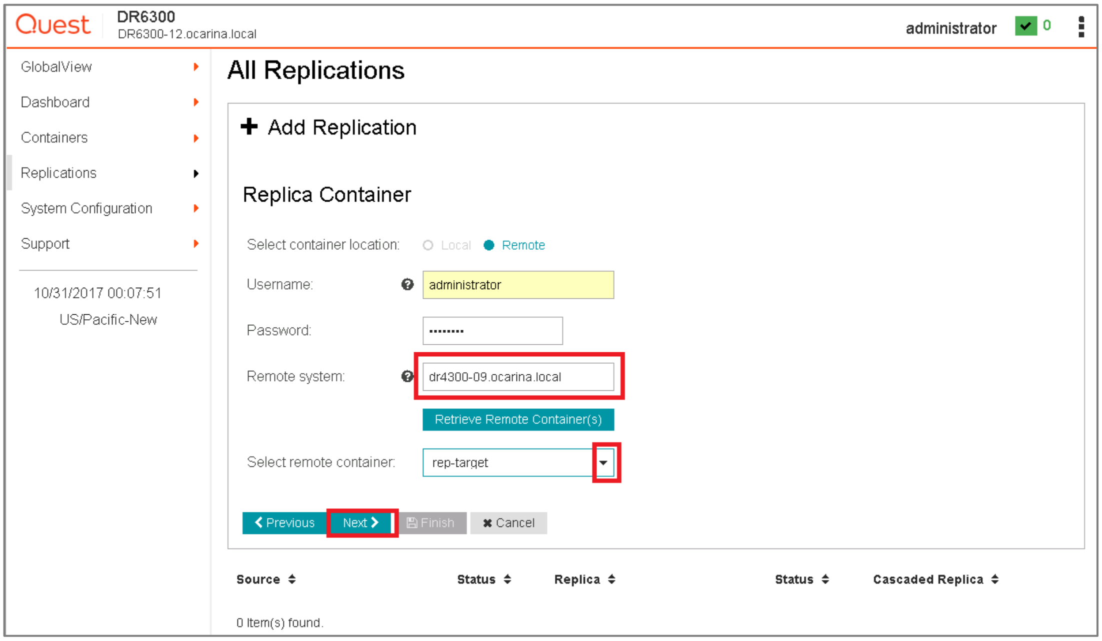


Encryption: ● Not Enabled ○ AES 128-bit ○ AES 256-bit

0 Item(s) found.

6 Select **Container from remote system**, enter the Target DR related information, click **Retrieve Containers**, select the populated target container from the list, and click **Create Replication.**

> NOTE: Enter credentials to authenticate to the target DR (default is “Administrator/St0r@ge!), click **Retrieve Containers**, and select the target container in the list.



Select container location: ○ Local ● Remote

Username: administrator

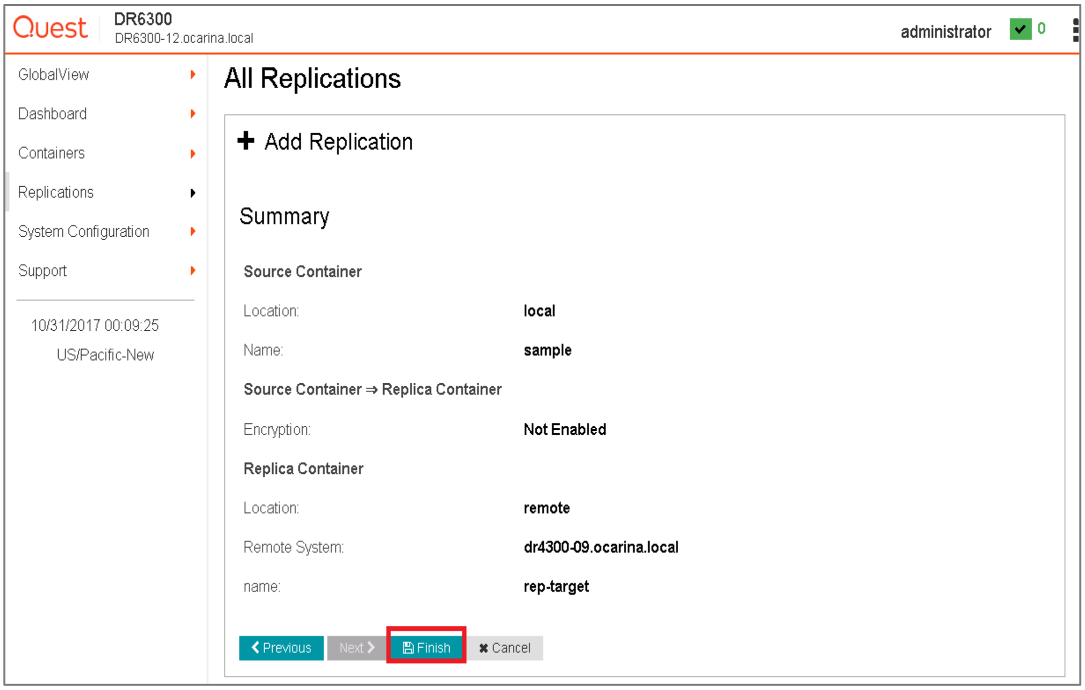
Password: ••••••••

Remote system: dr4300-09.ocarina.local

Select remote container: rep-target

0 Item(s) found.

7 Verify the summary and click **Finish**.



All Replications

Add Replication

Summary

Source Container

Location: local

Name: sample

Source Container ⇒ Replica Container

Encryption: Not Enabled

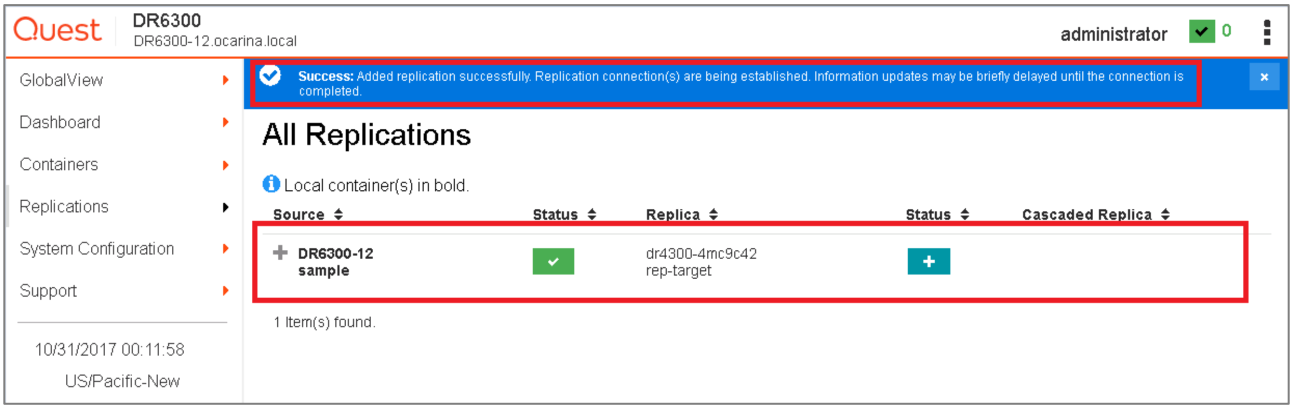
Replica Container

Location: remote

Remote System: dr4300-09.ocarina.local

name: rep-target

8 Verify that the replication is created successfully and make sure the **Status checkbox** is marked for the replication session.



Success: Added replication successfully. Replication connection(s) are being established. Information updates may be briefly delayed until the connection is completed.

All Replications

Local container(s) in bold.

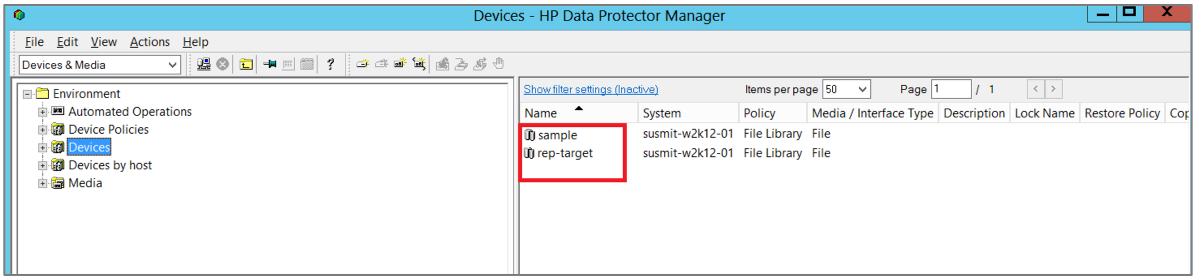
Source	Status	Replica	Status	Cascaded Replica
DR6300-12 **sample**	✓	dr4300-4mc9c42 rep-target	+	

1 Item(s) found.

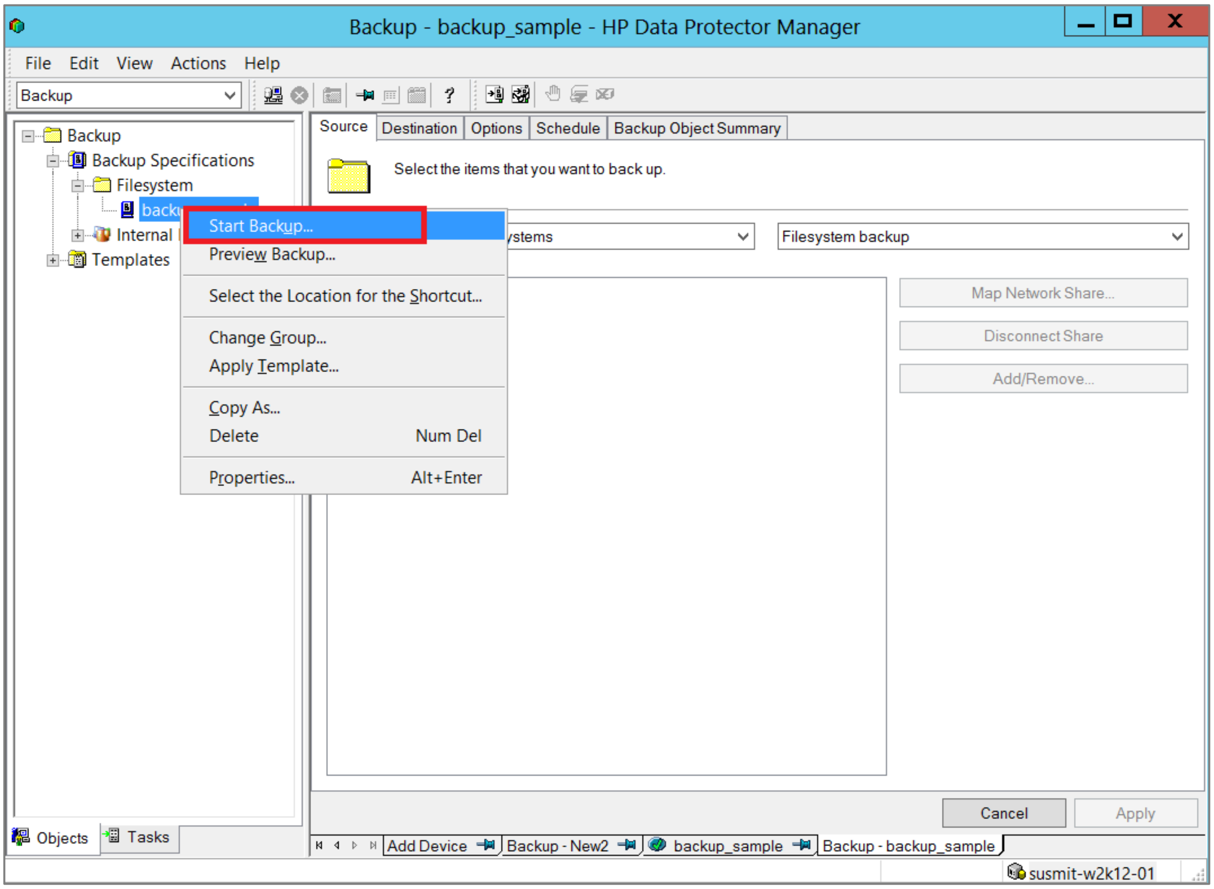
Runing backup to the source DR Series system (Optional)

This is needed only when there is no backup data on the source DR container.

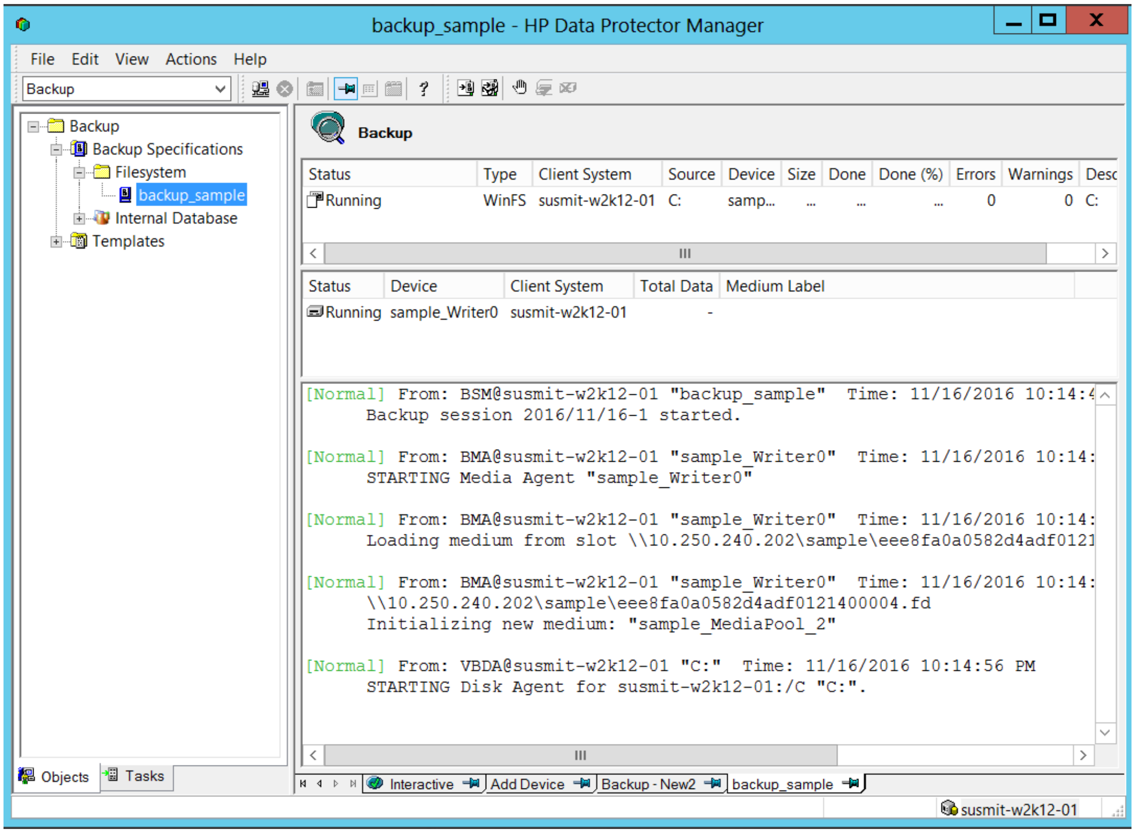
1 Add both source DR and target DR as Devices on HP DP, create a New Backup Job with source DR as the Target.



Name	System	Policy	Media / Interface Type	Description	Lock Name	Restore Policy	Cop
sample	susmit-w2k12-01	File Library	File				
rep-target	susmit-w2k12-01	File Library	File				



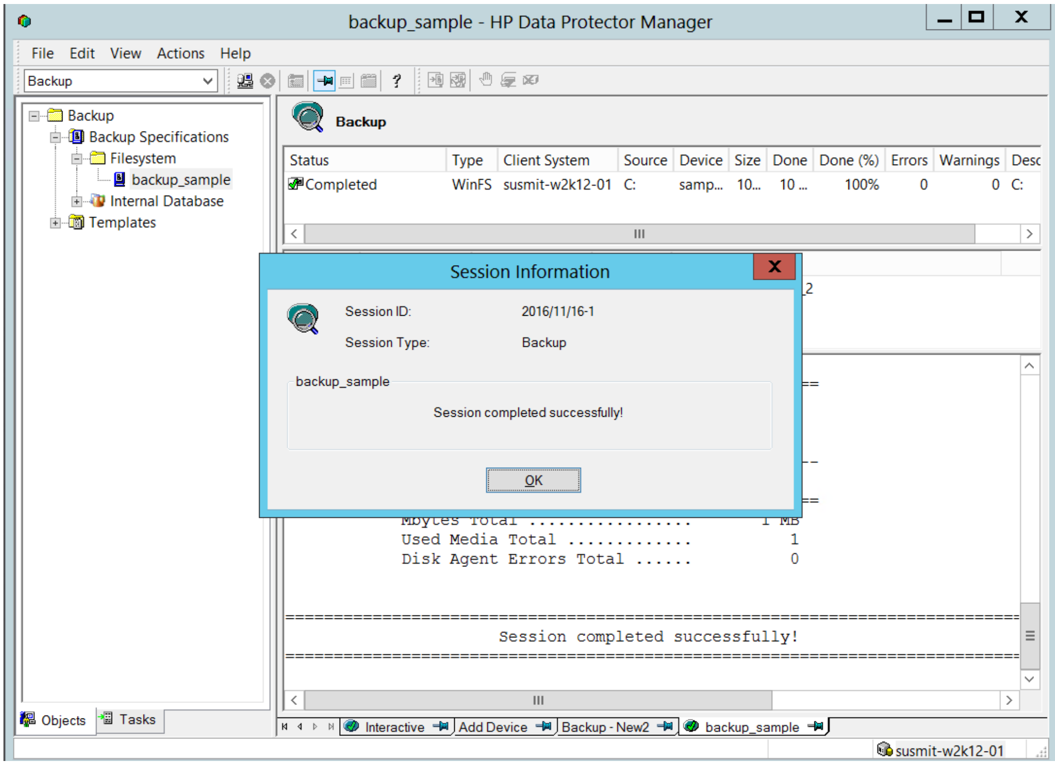
2 In the **Start Backup** window, click **OK** to start the backup using the appropriate settings, and monitor job status.



Status	Type	Client System	Source	Device	Size	Done	Done (%)	Errors	Warnings	Desc
Running	WinFS	susmit-w2k12-01	C:	samp...	...	...	...	0	0	C:

Status	Device	Client System	Total Data	Medium Label
Running	sample_Writer0	susmit-w2k12-01	-	

```
[Normal] From: BSM@susmit-w2k12-01 "backup_sample"  Time: 11/16/2016 10:14:4
      Backup session 2016/11/16-1 started.

[Normal] From: BMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/16/2016 10:14:
      STARTING Media Agent "sample_Writer0"

[Normal] From: BMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/16/2016 10:14:
      Loading medium from slot \\10.250.240.202\sample\eee8fa0a0582d4adf0121

[Normal] From: BMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/16/2016 10:14:
      \\10.250.240.202\sample\eee8fa0a0582d4adf0121400004.fd
      Initializing new medium: "sample_MediaPool_2"

[Normal] From: VBDA@susmit-w2k12-01 "C:"  Time: 11/16/2016 10:14:56 PM
      STARTING Disk Agent for susmit-w2k12-01:/C "C:".
```



Backup

Status	Type	Client System	Source	Device	Size	Done	Done (%)	Errors	Warnings	Desc
Completed	WinFS	susmit-w2k12-01	C:	samp...	10...	10 ...	100%	0	0	C:

Session Information

Session ID: 2016/11/16-1

Session Type: Backup

backup_sample

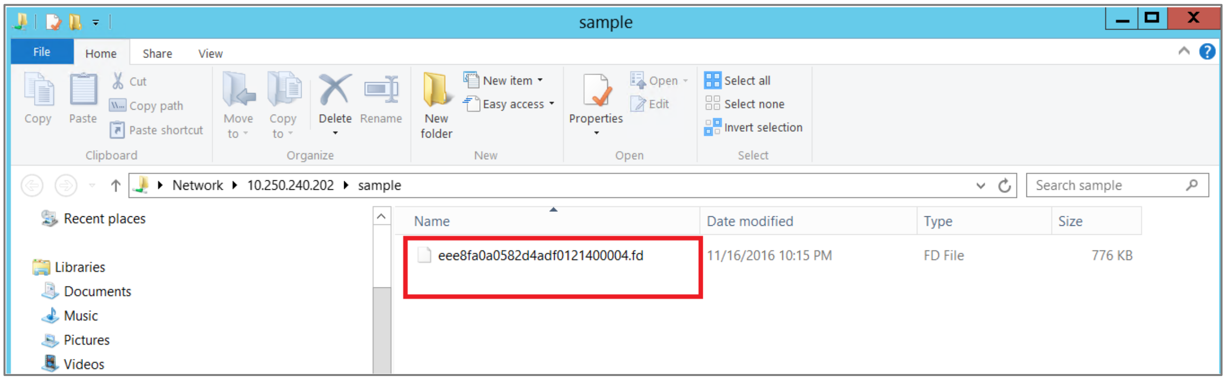
Session completed successfully!

OK

```
        Mbytes Total ................     1 MB
        Used Media Total ............        1
        Disk Agent Errors Total ......       0

==========================================================================
                    Session completed successfully!
==========================================================================
```

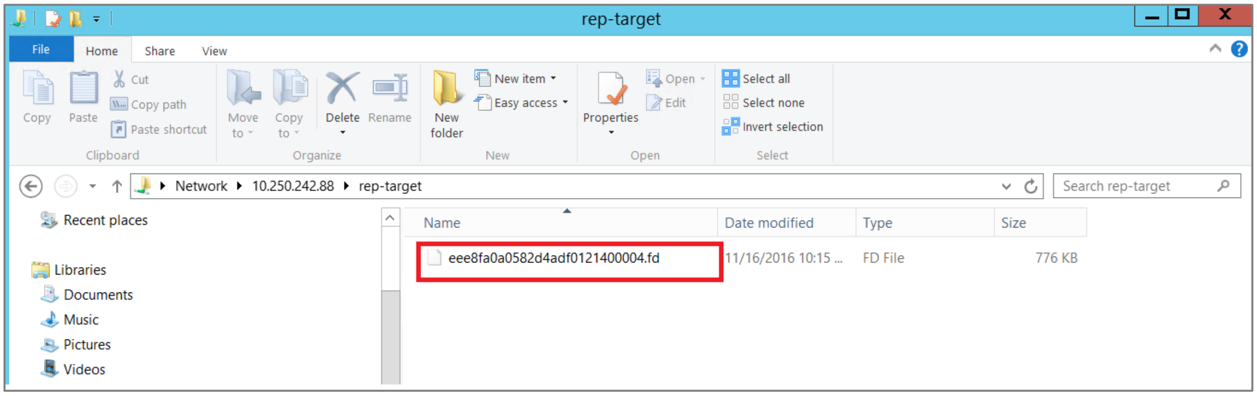
When the backup job is completed, HP Data Protector creates backup files using the suffix '.fd' on source DR, and the '.fd' files will be replicated to the target DR, as shown below.

Source DR:


sample
File Home Share View
Copy Paste Cut Copy path Paste shortcut
Clipboard
Move to Copy to Delete Rename
Organize
New item Easy access New folder
New
Properties Open Edit
Open
Select all Select none Invert selection
Select
Network ▸ 10.250.240.202 ▸ sample
Search sample
Recent places
Libraries
Documents
Music
Pictures
Videos

Name	Date modified	Type	Size
eee8fa0a0582d4adf0121400004.fd	11/16/2016 10:15 PM	FD File	776 KB

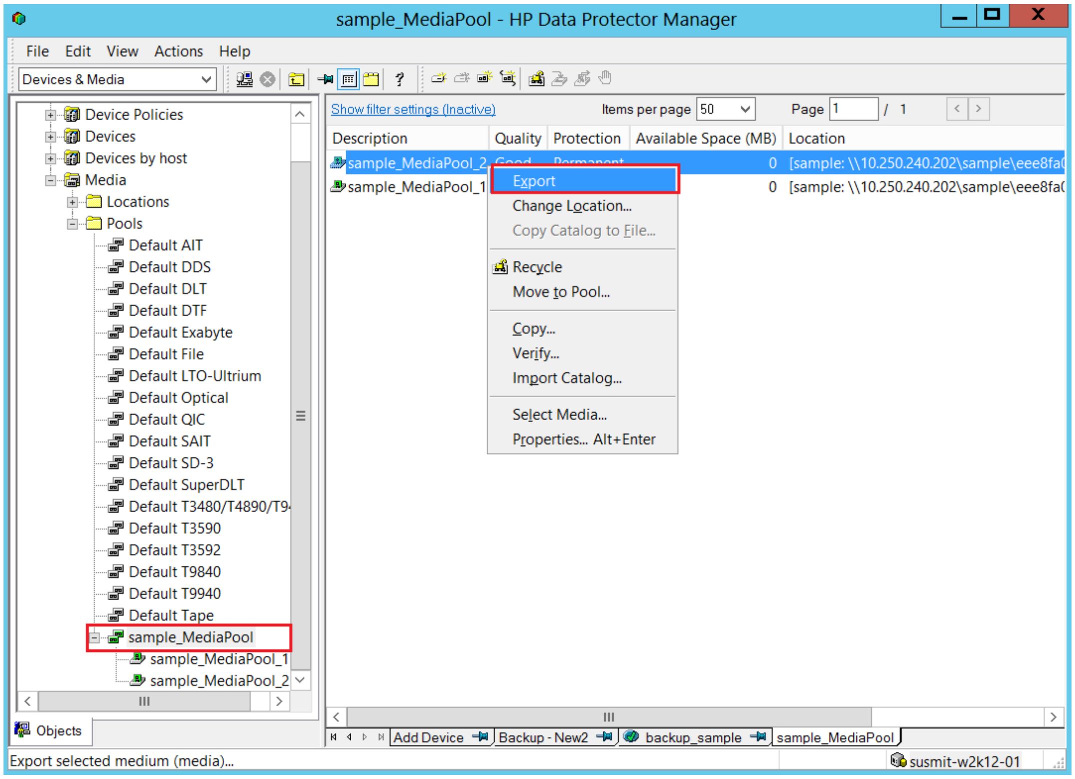
Target DR:



Name	Date modified	Type	Size
eee8fa0a0582d4adf0121400004.fd	11/16/2016 10:15 ...	FD File	776 KB

Preparing the replication target for restore

1 In HP Data Protector, go to Devices & Media > Media > Pools, right-click the Media Pool associated with the source container device and the backup set that needs to be restored, and click **Export**.

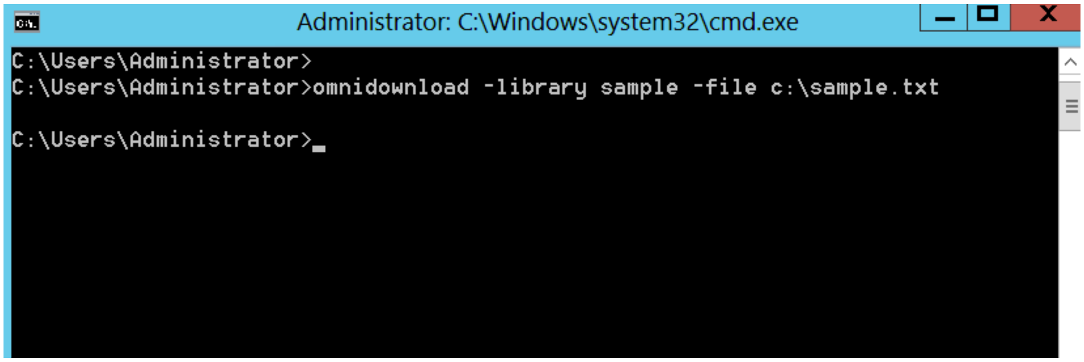


Description	Quality	Protection	Available Space (MB)	Location
sample_MediaPool_2	Good	Permanent	0	[sample: \\10.250.240.202\sample\eee8fa(
sample_MediaPool_1			0	[sample: \\10.250.240.202\sample\eee8fa(

Export selected medium (media)...

NOTE: If the media pool is protected and cannot be exported, you should perform **Recycle** before **Export**

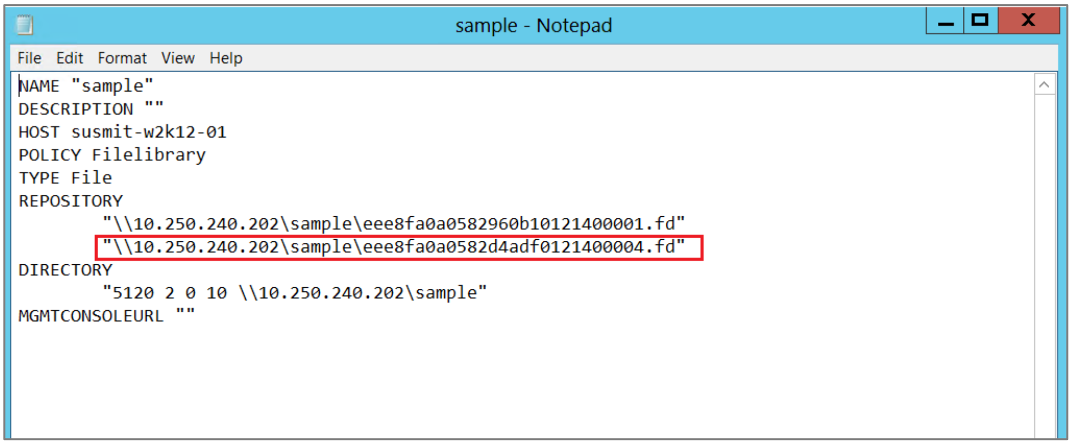
2 Open the HP Data Protector CLI console, and use the command utility **“omnidownload”** to download the source container library configuration from IDB.



```
C:\Users\Administrator>
C:\Users\Administrator>omnidownload -library sample -file c:\sample.txt

C:\Users\Administrator>_
```

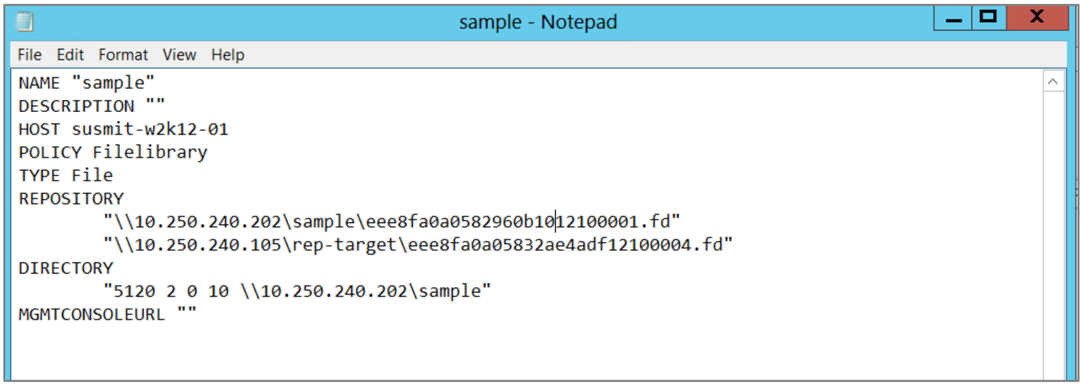
NOTE: Refer to Appendix C for information about how to use the command “**omnidownload**”.

3 Edit the file, modify or add the object information to point to the target DR Series system, and save this file.



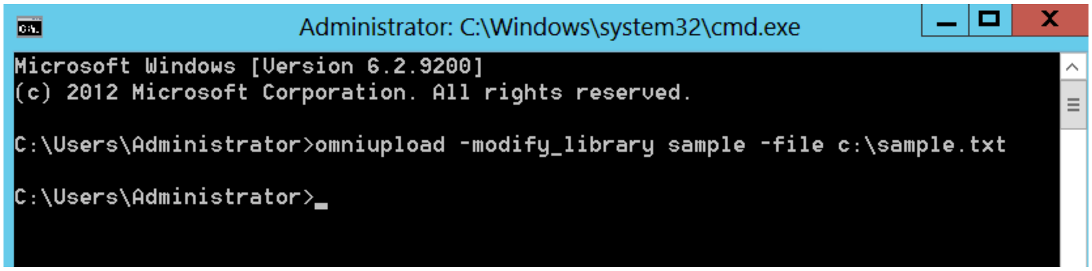
```
NAME "sample"
DESCRIPTION ""
HOST susmit-w2k12-01
POLICY Filelibrary
TYPE File
REPOSITORY
        "\\10.250.240.202\sample\eee8fa0a0582960b10121400001.fd"
        "\\10.250.240.202\sample\eee8fa0a0582d4adf0121400004.fd"
DIRECTORY
        "5120 2 0 10 \\10.250.240.202\sample"
MGMTCONSOLEURL ""
```

4 Modify the file with the target DR Series system information.



```
NAME "sample"
DESCRIPTION ""
HOST susmit-w2k12-01
POLICY Filelibrary
TYPE File
REPOSITORY
        "\\10.250.240.202\sample\eee8fa0a0582960b1012100001.fd"
        "\\10.250.240.105\rep-target\eee8fa0a05832ae4adf12100004.fd"
DIRECTORY
        "5120 2 0 10 \\10.250.240.202\sample"
MGMTCONSOLEURL ""
```

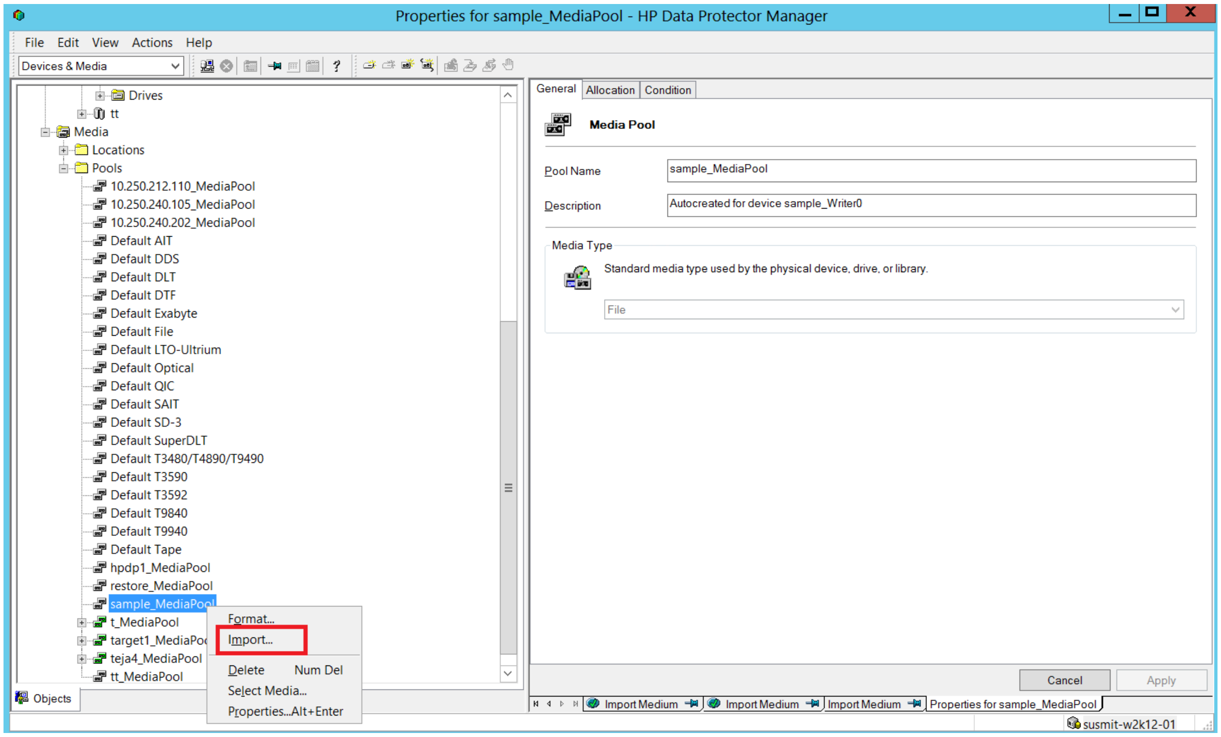
5 Upload this modified configuration file to IDB using the command “**omniupload**”.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>omniupload -modify_library sample -file c:\sample.txt

C:\Users\Administrator>_
```

NOTE: Refer to Appendix C for information on how to use the command “**omniupload**”.

6 Click **Media > Pools > Import** to import the device object from the target device.



Media Pool

Pool Name: sample_MediaPool

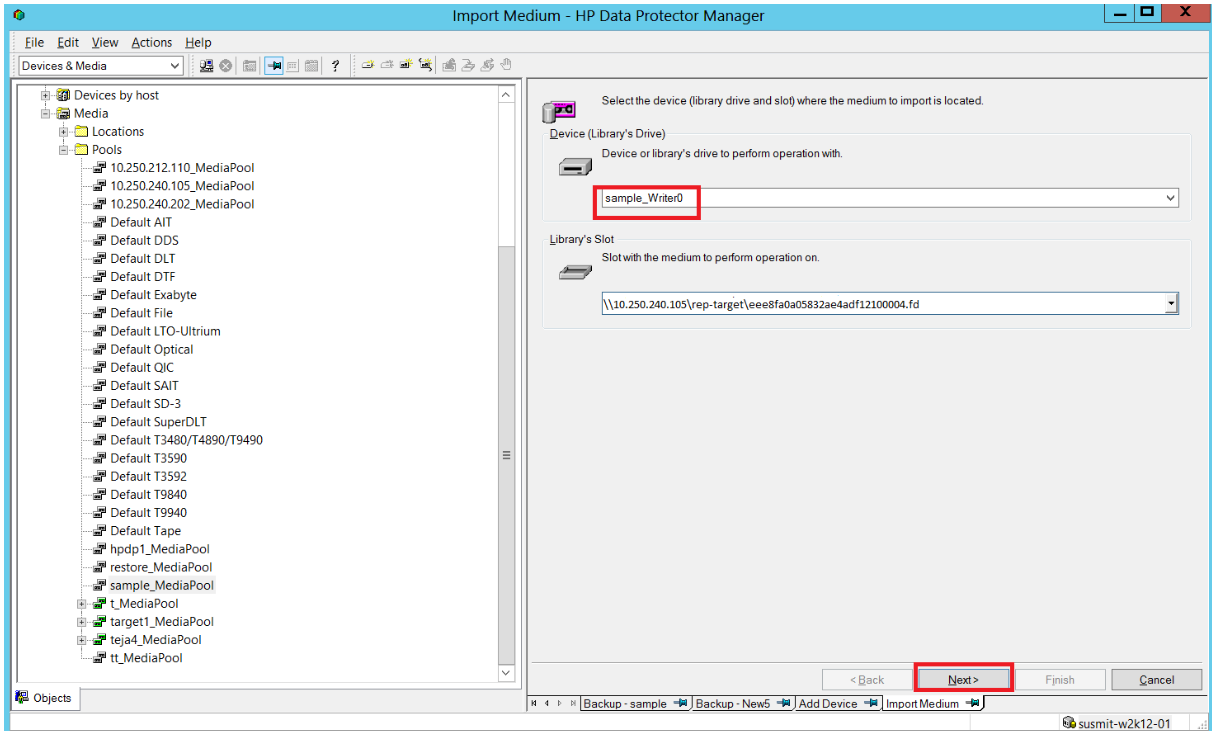
Description: Autocreated for device sample_Writer0

Media Type

Standard media type used by the physical device, drive, or library.

File

7 Click **Next**.



Select the device (library drive and slot) where the medium to import is located.

Device (Library's Drive)

Device or library's drive to perform operation with.

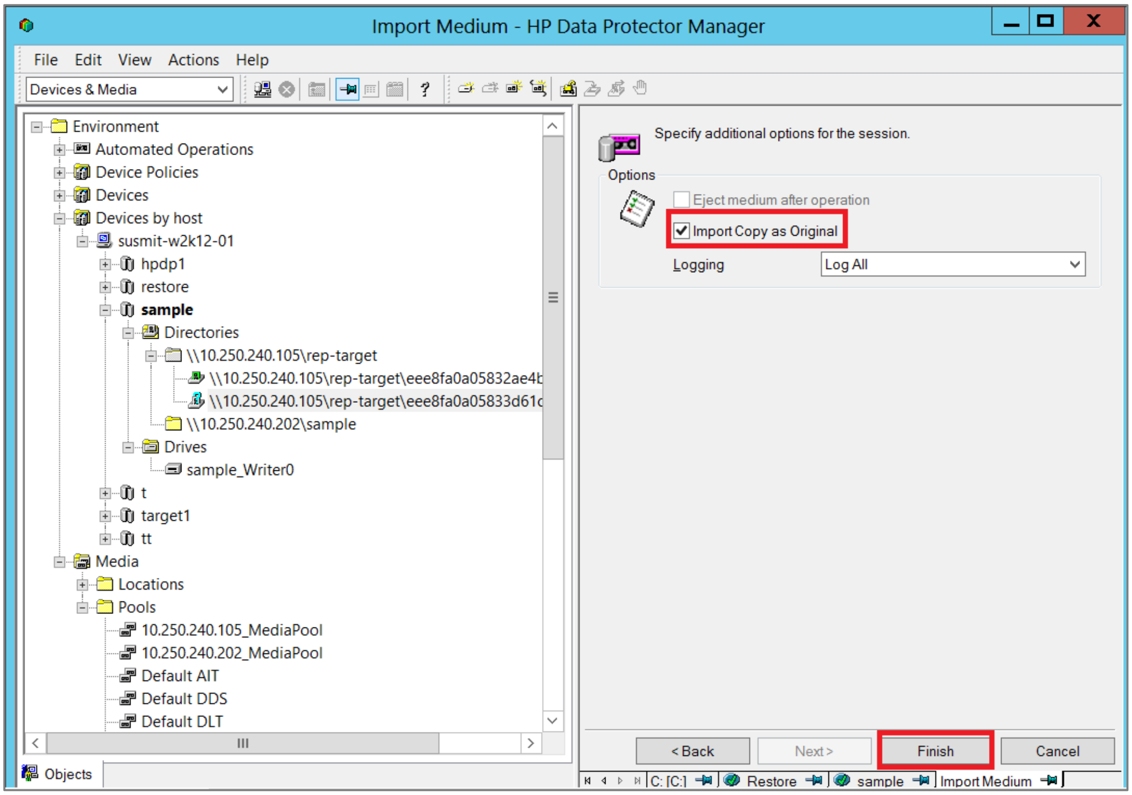
sample_Writer0

Library's Slot

Slot with the medium to perform operation on.

\\10.250.240.105\rep-target\eee8fa0a05832ae4adf12100004.fd

8 Select the **Import Copy as Original** checkbox, and click **Finish**.



Specify additional options for the session.

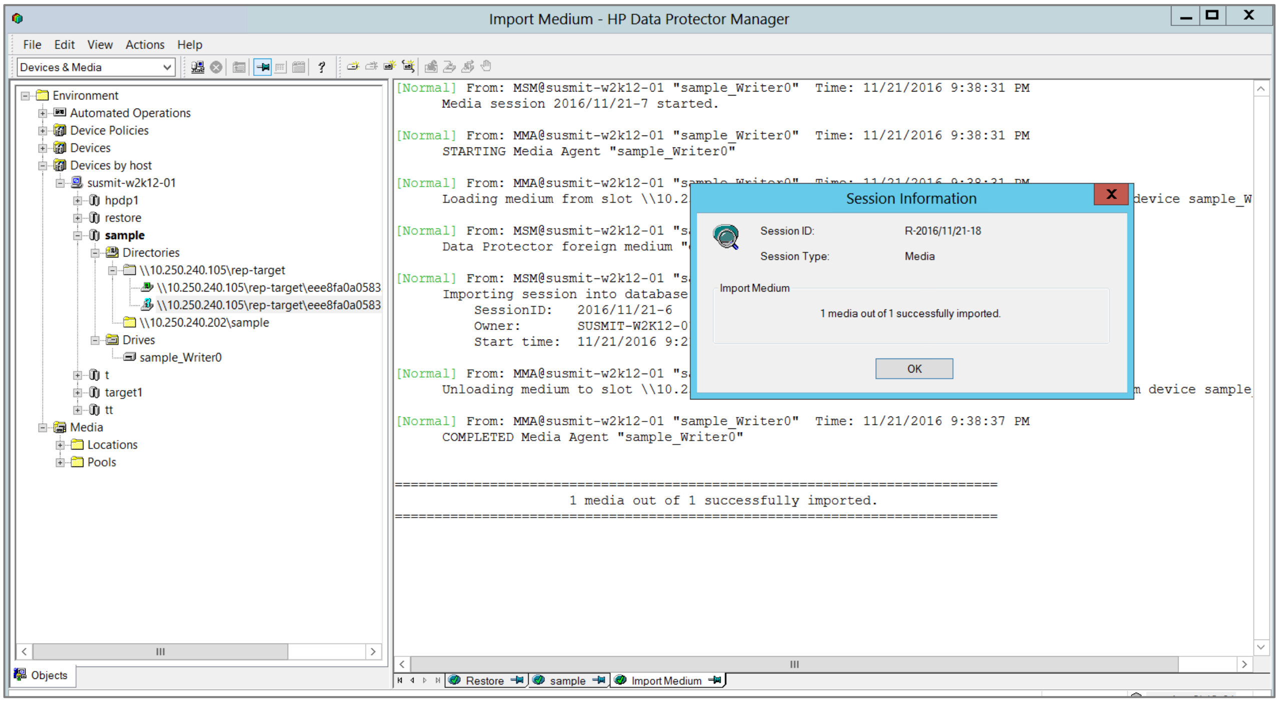
Options

☐ Eject medium after operation

☑ Import Copy as Original

Logging: Log All

9 Verify that the import is done successfully.



```
[Normal] From: MSM@susmit-w2k12-01 "sample_Writer0"  Time: 11/21/2016 9:38:31 PM
      Media session 2016/11/21-7 started.

[Normal] From: MMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/21/2016 9:38:31 PM
      STARTING Media Agent "sample_Writer0"

[Normal] From: MMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/21/2016 9:38:31 PM
      Loading medium from slot \\10.2                                    device sample_W

[Normal] From: MSM@susmit-w2k12-01 "s
      Data Protector foreign medium "

[Normal] From: MSM@susmit-w2k12-01 "s
      Importing session into database
          SessionID:    2016/11/21-6
          Owner:        SUSMIT-W2K12-0
          Start time:   11/21/2016 9:2

[Normal] From: MMA@susmit-w2k12-01 "s
      Unloading medium to slot \\10.2                                    m device sample

[Normal] From: MMA@susmit-w2k12-01 "sample_Writer0"  Time: 11/21/2016 9:38:37 PM
      COMPLETED Media Agent "sample_Writer0"


=============================================================================
                      1 media out of 1 successfully imported.
=============================================================================
```

Session Information

Session ID: R-2016/11/21-18

Session Type: Media

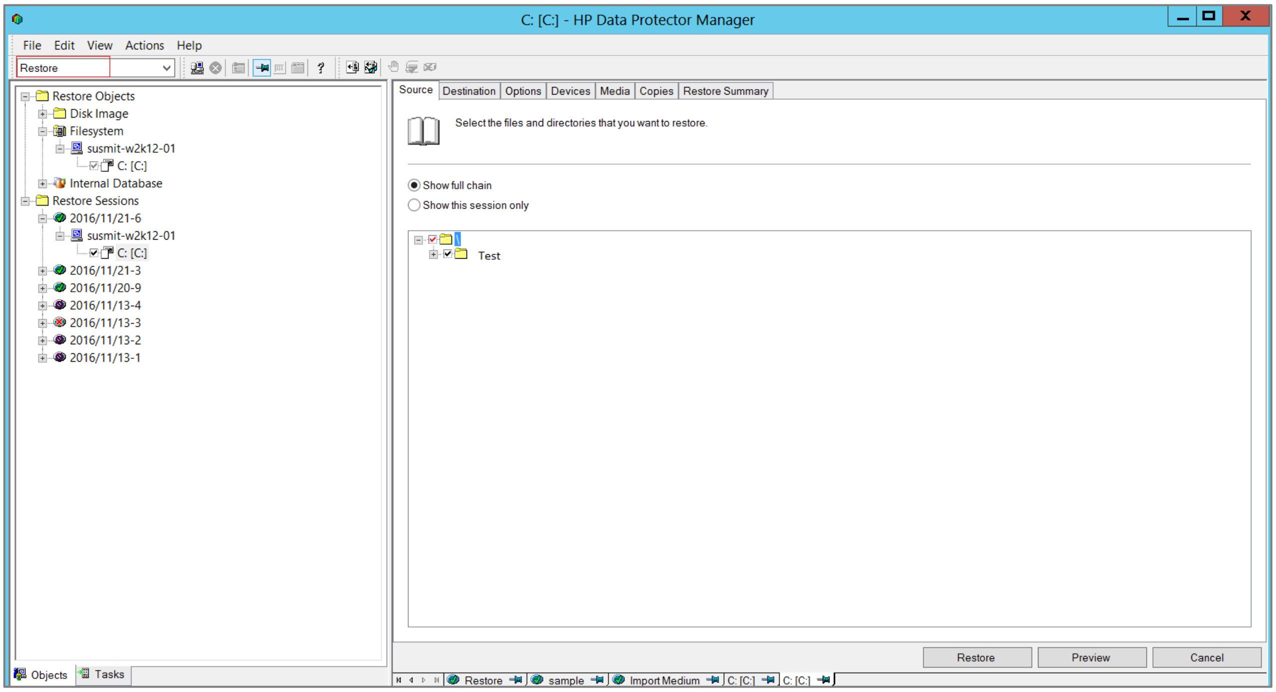
Import Medium

1 media out of 1 successfully imported.

OK

Restoring from the target DR Series system

1 In the **Context List** drop-down menu, select **Restore**, run the restore session that is associated to the backup set, and click **Restore**.



C: [C:] - HP Data Protector Manager

Restore

- Restore Objects
  - Disk Image
  - Filesystem
    - susmit-w2k12-01
      - ☑ C: [C:]
  - Internal Database
- Restore Sessions
  - 2016/11/21-6
    - susmit-w2k12-01
      - ☑ C: [C:]
  - 2016/11/21-3
  - 2016/11/20-9
  - 2016/11/13-4
  - 2016/11/13-3
  - 2016/11/13-2
  - 2016/11/13-1

Select the files and directories that you want to restore.

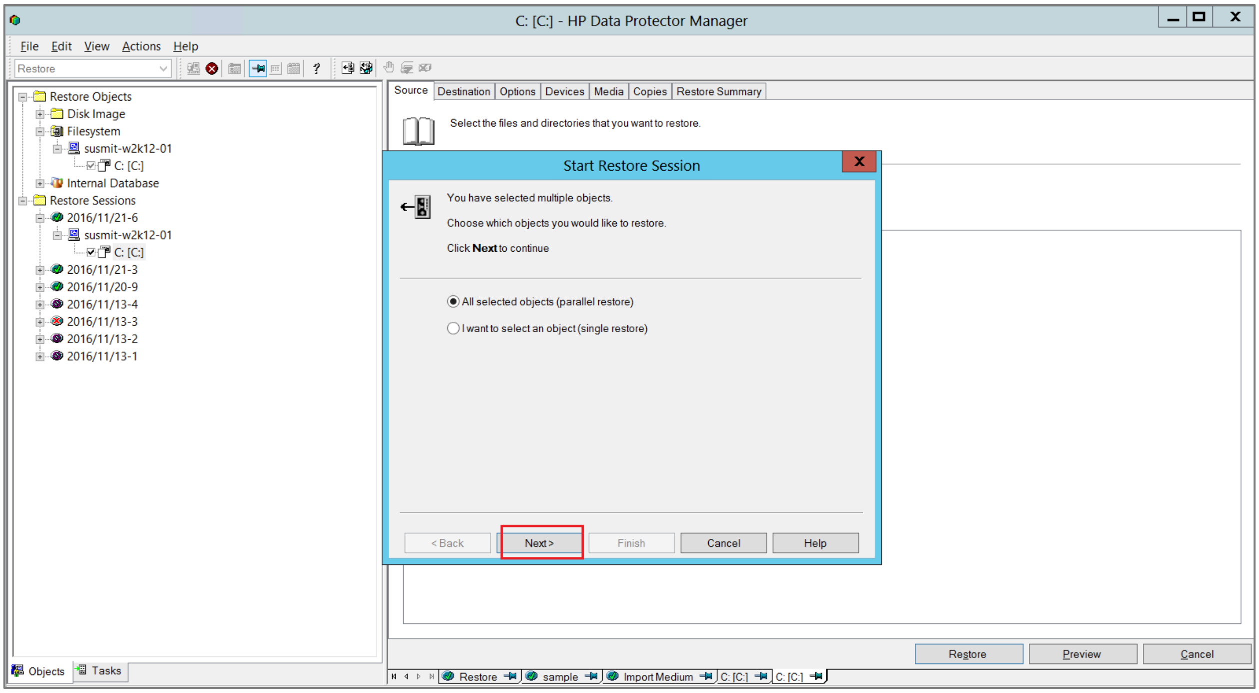
● Show full chain

○ Show this session only

☑ \
- ☑ Test

File Edit View Actions Help
Source Destination Options Devices Media Copies Restore Summary
Restore Preview Cancel
Objects Tasks
Restore sample Import Medium C: [C:] C: [C:]

2 Click **Next**.



C: [C:] - HP Data Protector Manager

Select the files and directories that you want to restore.

Start Restore Session

You have selected multiple objects.

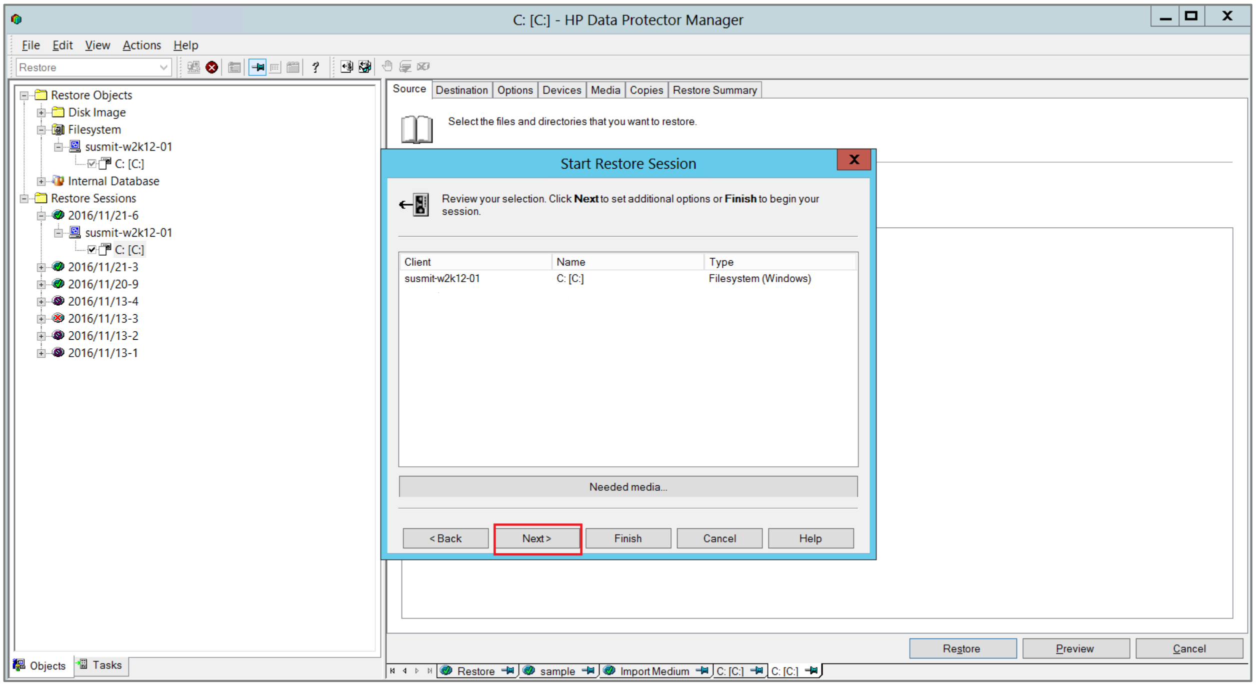
Choose which objects you would like to restore.

Click **Next** to continue

● All selected objects (parallel restore)

○ I want to select an object (single restore)

3 Click **Next**.

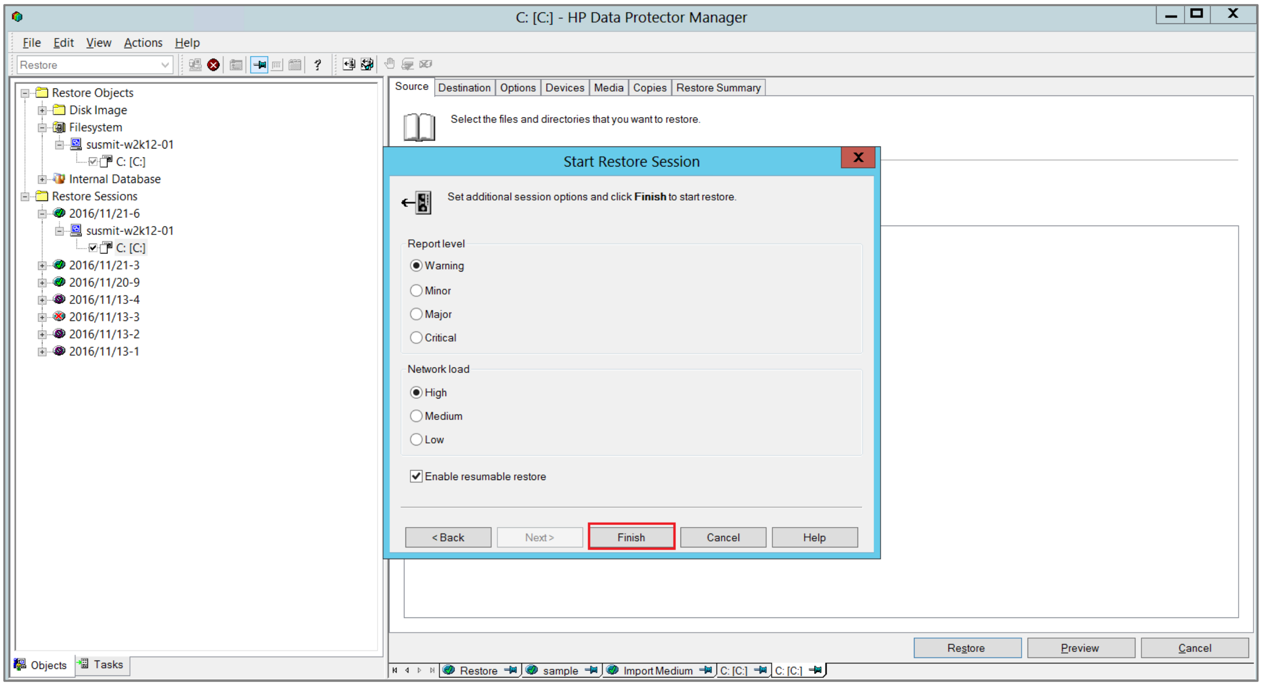


Select the files and directories that you want to restore.

Review your selection. Click **Next** to set additional options or **Finish** to begin your session.

Client	Name	Type
susmit-w2k12-01	C: [C:]	Filesystem (Windows)

4 Click **Finish**.



Select the files and directories that you want to restore.

Set additional session options and click **Finish** to start restore.

Report level

● Warning

○ Minor

○ Major

○ Critical

Network load

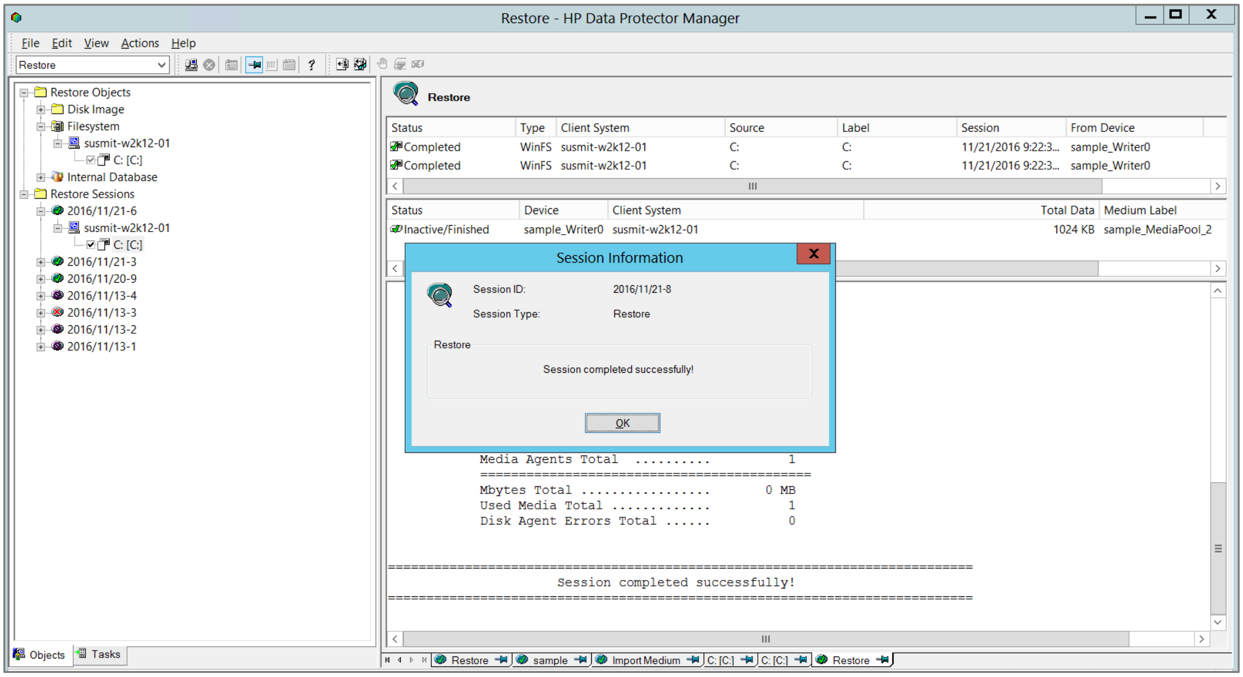
● High

○ Medium

○ Low

☑ Enable resumable restore

5 Verify that the restore is done successfully.



Status	Type	Client System	Source	Label	Session	From Device
Completed	WinFS	susmit-w2k12-01	C:	C:	11/21/2016 9:22:3...	sample_Writer0
Completed	WinFS	susmit-w2k12-01	C:	C:	11/21/2016 9:22:3...	sample_Writer0

Status	Device	Client System	Total Data	Medium Label
Inactive/Finished	sample_Writer0	susmit-w2k12-01	1024 KB	sample_MediaPool_2

Session Information

Session ID: 2016/11/21-8

Session Type: Restore

Restore

Session completed successfully!

```
            Media Agents Total  ..........          1
            ============================================
            Mbytes Total .................       0 MB
            Used Media Total .............          1
            Disk Agent Errors Total ......          0


==============================================================================
                     Session completed successfully!
==============================================================================
```

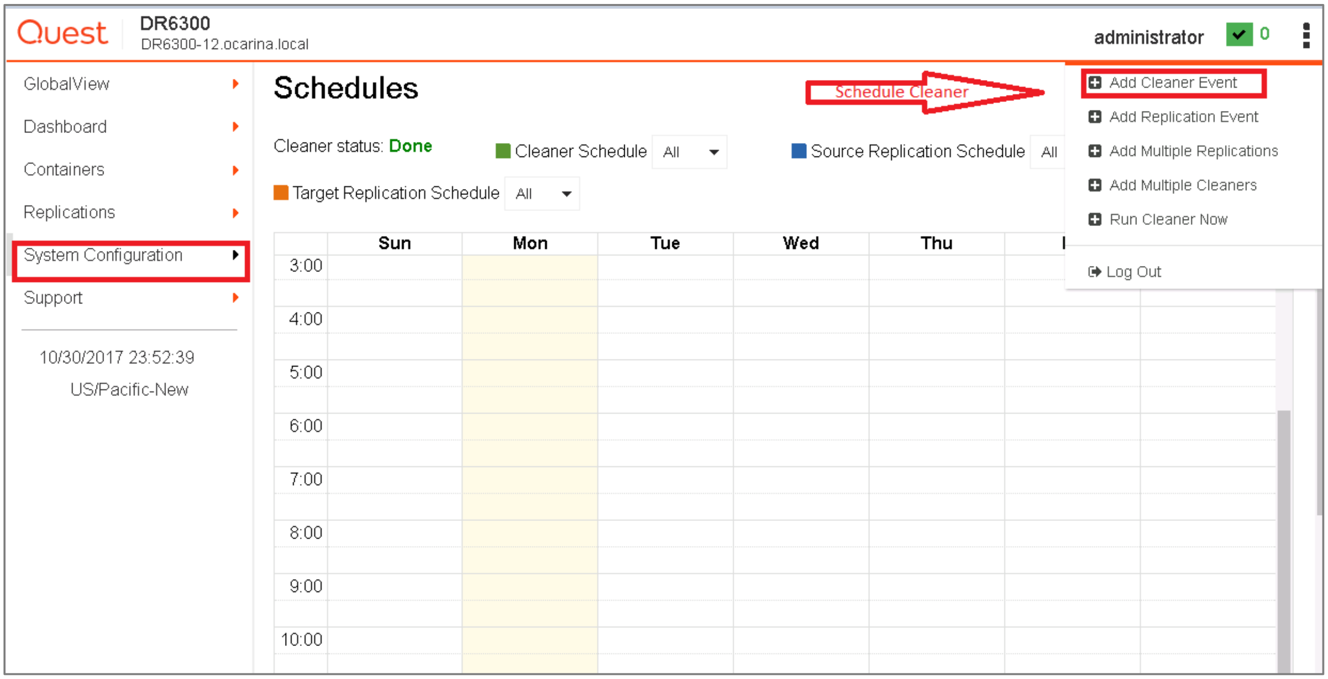
5

Setting up the DR Series system cleaner

The cleaner will run during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner which will force it to run during that scheduled time.

If necessary, you can do the following procedure as described in the screenshot to force the cleaner to run. Once all the backup jobs are setup the DR Series System cleaner can be scheduled. The DR Series System cleaner should run at least 40 hours per week when backups are not taking place, generally after a backup job has completed.

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication.



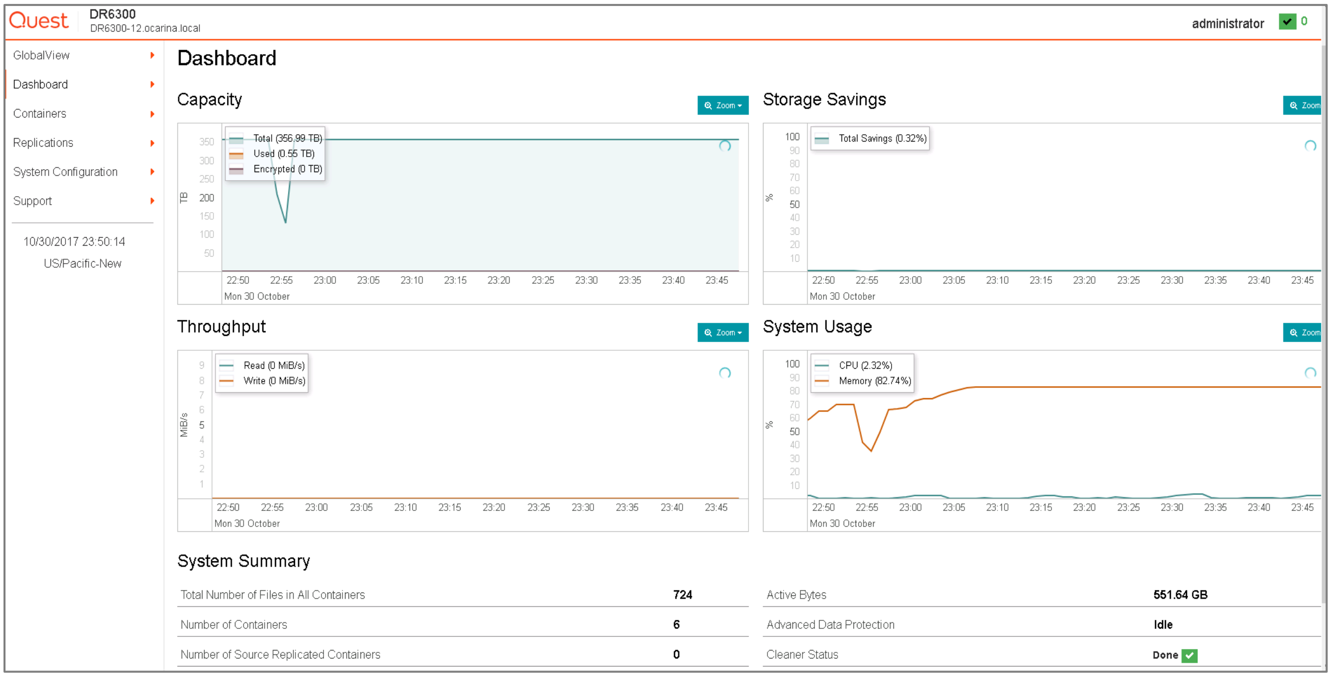
Cleaner status: Done

6

Monitoring Deduplication, Compression and Performance

After backup jobs have completed, the DR Series system tracks capacity, storage savings and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits of the DR Series System.

NOTE: Deduplication ratios increase over time; it is not uncommon to see a 2-4x reduction (25-50% total savings) on the initial backup. As additional full backup jobs complete, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio in most cases.



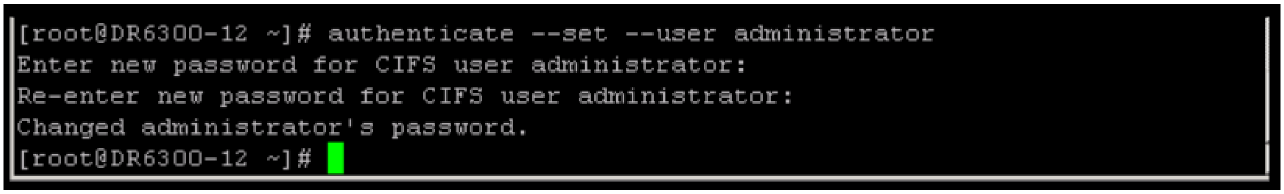
Total Number of Files in All Containers	**724**	Active Bytes	**551.64 GB**
Number of Containers	**6**	Advanced Data Protection	**Idle**
Number of Source Replicated Containers	**0**	Cleaner Status	**Done** ✓

Appendices

A - Creating a storage device for CIFS

There are two options for HP Data Protector to authenticate to the DR Series system through CIFS.

- **DR joined into the domain**: Integrates HP Data Protector Server and DR Series System with Active Directory
    - Ensure the AD user has appropriate ACLs to the DR Series System Container share.
    - Set the HP Data Protector service to run with this AD user <Domain\User>.
- **DR as a standalone CIFS server**: Make sure the HP Data Protector Inet service and CRS service use the same logon user. Make sure the DR Series system also has the same username and password defined in the Local Workgroup Users. Also, make sure this CIFS user has appropriate access permission to the DR Series System container share. HP Data Protector services will use this user to authenticate to the DR Series System share in Workgroup mode.
    - To set the password for the local CIFS administrator on the DR Series System, log on to the DR using SSH.
        - Log on with username: administrator, and password: St0r@ge!
        - Run the following command: authenticate --set --user administrator

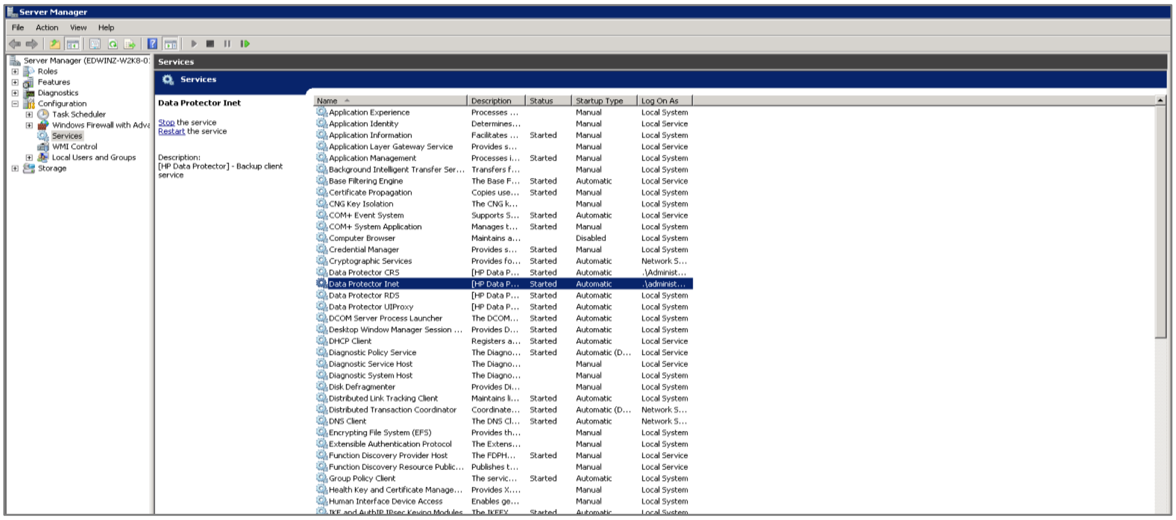


```
[root@DR6300-12 ~]# authenticate --set --user administrator
Enter new password for CIFS user administrator:
Re-enter new password for CIFS user administrator:
Changed administrator's password.
[root@DR6300-12 ~]# 
```

> **NOTE:** The CIFS administrator account is a separate account from the administrator account used to administer the appliance. After an authentication method is chosen, set the HP Data Protector Service account to use the CIFS administrator account.

1 Launch the Microsoft Services Snap-in by clicking **Start** > **Run** > **Services.msc** > **Enter**.

2 Locate the Data Protector Inet and Data Protector CRS Service, right-click **Properties** and click the Log On tab.



Data Protector Inet

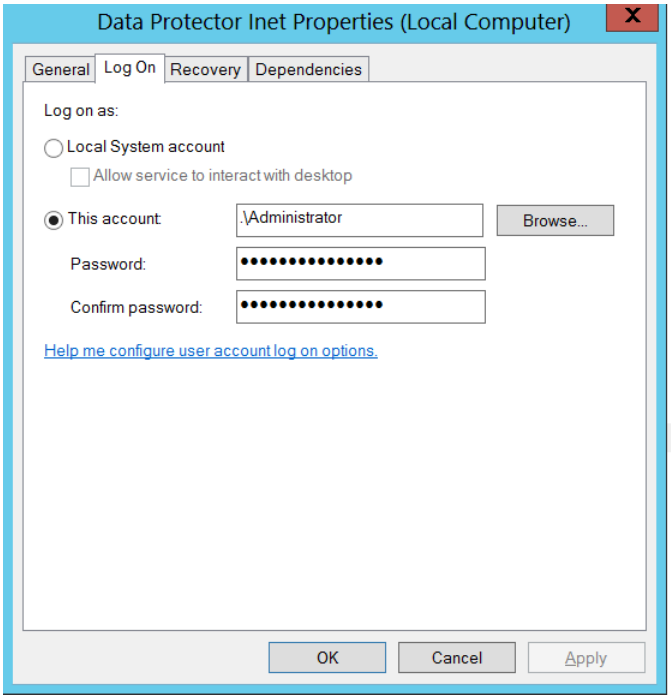
Stop the service
Restart the service

Description:
[HP Data Protector] - Backup client service

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes ...		Manual	Local System
Application Identity	Determines...		Manual	Local Service
Application Information	Facilitates ...	Started	Manual	Local System
Application Layer Gateway Service	Provides s...		Manual	Local Service
Application Management	Processes i...	Started	Manual	Local System
Background Intelligent Transfer Ser...	Transfers f...		Manual	Local System
Base Filtering Engine	The Base F...	Started	Automatic	Local Service
Certificate Propagation	Copies use...	Started	Manual	Local System
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Application	Manages t...	Started	Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Credential Manager	Provides s...	Started	Manual	Local System
Cryptographic Services	Provides fo...	Started	Automatic	Network S...
Data Protector CRS	[HP Data P...	Started	Automatic	.\Administ...
Data Protector Inet	[HP Data P...	Started	Automatic	.\administ...
Data Protector RDS	[HP Data P...	Started	Automatic	Local System
Data Protector UIProxy	[HP Data P...	Started	Automatic	Local System
DCOM Server Process Launcher	The DCOM...	Started	Automatic	Local System
Desktop Window Manager Session ...	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Started	Automatic (D...	Local Service
Diagnostic Service Host	The Diagno...		Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local System
Disk Defragmenter	Provides Di...		Manual	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...	Started	Automatic (D...	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...
Encrypting File System (EFS)	Provides th...		Manual	Local System
Extensible Authentication Protocol	The Extens...		Manual	Local System
Function Discovery Provider Host	The FDPH...	Started	Manual	Local Service
Function Discovery Resource Public...	Publishes t...		Manual	Local Service
Group Policy Client	The servic...	Started	Automatic	Local System
Health Key and Certificate Manage...	Provides X....		Manual	Local System
Human Interface Device Access	Enables ge...		Manual	Local System
IKE and AuthIP IPsec Keying Modules	The IKEEX...	Started	Automatic	Local System

NOTE: Do this step only when no backups are currently running, as restarting the services causes backup jobs to fail. Double-click on the services one at a time.

If you are using local synced accounts rather than the AD account, make sure that there is a ".\" in front of the user name.



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\Administrator

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

3 Click **OK**.

4 After changing both services for HP Data Protector, select **Stop/Start** to restart the two services.

B - Creating a storage device for NFS

For NFS backup using HP Data Protector, a target folder needs to be created as an NFS share directory. This is the location to which backup objects will be written. (This is not required for adding a CIFS share.)

1 Mount the DR Series System NFS share onto the NFS share directory to which backup objects will be written in the HP Data Protector environment.

2 Verify the NFS share. (One way is to try using the Linux command “cat /proc/mounts”. The rsize and wsize of the nfs mount should be 512K.)

C - User commands

- **Omnidownload**
  - Downloads information about a backup device and a library from the Data Protector Internal Database (IDB).
  - This command is available on systems with the Data Protector User Interface component installed.

    Examples:

    To review the information about a virtual tape library named "VTL" in ASCII format that will be saved as the file "libVTL.txt" to the directory "C:\Temp", run:

    omnidownload -library VTL -file C:\Temp\libVTL.txt

- **Omniupload**
  - Uploads information about a backup device from an ASCII file to the Data Protector internal database(IDB).
  - This command is available on systems with the Data Protector User Interface component installed.

    Examples:

    To modify library"Exabyte1" using the information in the file "/tmp/EXA", run:

    omniupload -modify_library Exabyte1 -file /tmp/EXA