

Setting up the DR Series System as an Archive Target on AppAssure 6.2

Technical White Paper

Quest Engineering

October 2017



© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

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 OF ANY 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.

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

Setting Up the Quest™ DR Series System as an Archive Target on AppAssure 6.2

Updated – November 13, 2017

Contents

Installing and configuring the DR Series system.....	6
Setting up AppAssure	13
Archiving backup images to the DR Series system	13
Restoring archived backup images from the DR Series system.....	28
Setting up the DR Series system cleaner	31
Monitoring deduplication, compression, and performance	33
Appendices	34
A - Configuring the DR container share as a CIFS storage device.....	34
B - Backing up a Linux client.....	35
Installing the Linux agent	35
Configuring the Linux client machine	36

Revisions

Date	Description
January 2014	Initial release
November 2016	Updated with new DR Series system GUI screenshots (version 4.0)
October 2017	Updated with new DR Series system GUI post-rebranding (version 4.0.3)

Executive Summary

This paper provides information about how to set up the DR Series system as a backup target for Quest AppAssure.

For additional information, see the DR Series system documentation and other data management application best practices whitepapers for your specific DR Series system at:

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

For more information about AppAssure, refer to the Quest AppAssure documentation at:

<https://support.quest.com/appassure>



NOTE: The DR Series system/ AppAssure build version and screenshots used in this document may vary slightly, depending on the version of the DR Series system/ AppAssure Software version you are using.

Installing and configuring the DR Series system

Follow these steps to install and configure the DR Series system.

- 1 Rack and cable the DR Series system and power it on.
- 2 Initialize the DR Series system. Refer to the Quest DR Series System Administrator Guide under the following topics: “iDRAC Connection,” “Logging in and Initializing the DR Series System,” and “Accessing iDRAC6/iDRAC7 Using RACADM”.
- 3 Log on to iDRAC using the default address **192.168.0.120**, or the IP assigned to the iDRAC interface. Use the user name and password of **“root/calvin”**.

INTEGRATED REMOTE ACCESS CONTROLLER Enterprise

Login

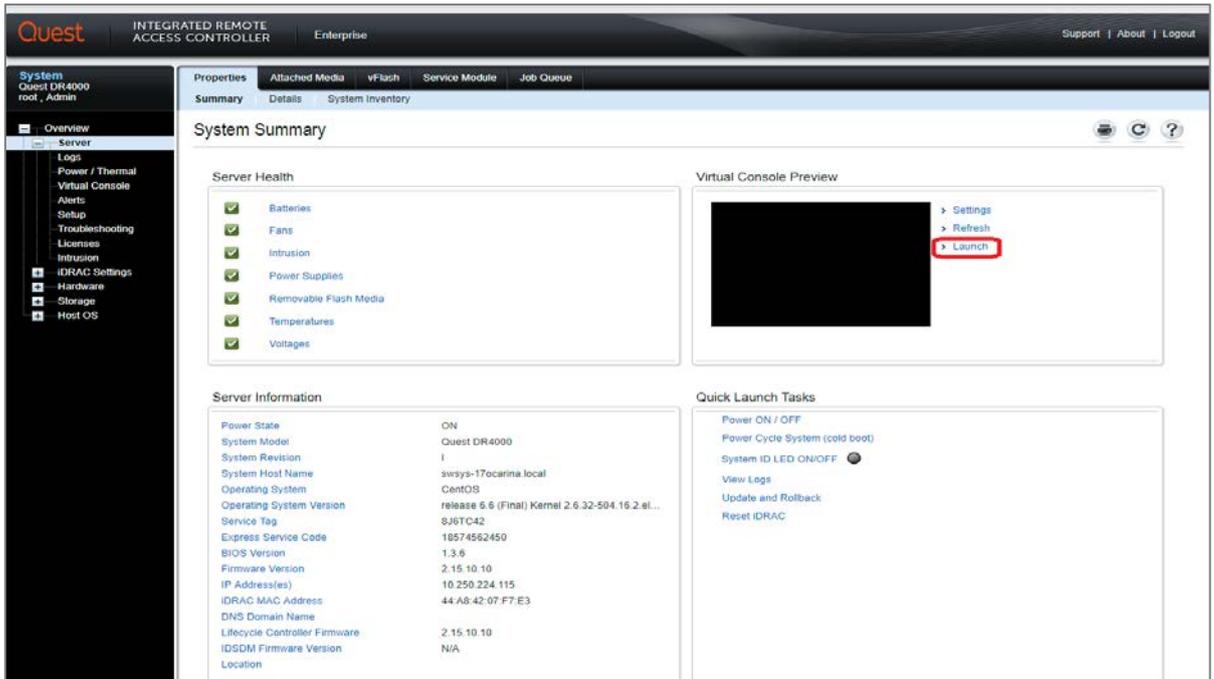
IDRAC | Quest DR4000

Type the Username and Password and click Submit.

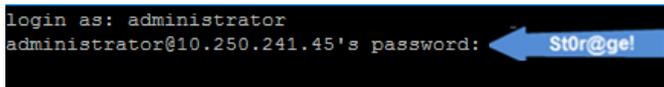
Username: Password:

Domain:

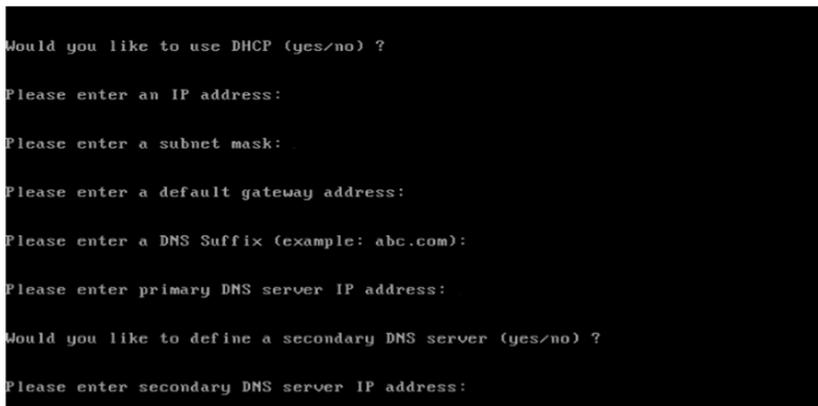
- 4 Launch the virtual console.



- 5 After the virtual console is open, log in to the system as user administrator and the password **St0r@ge!** (the "0" in the password is the numeral zero).



- 6 Set the user-defined networking preferences.

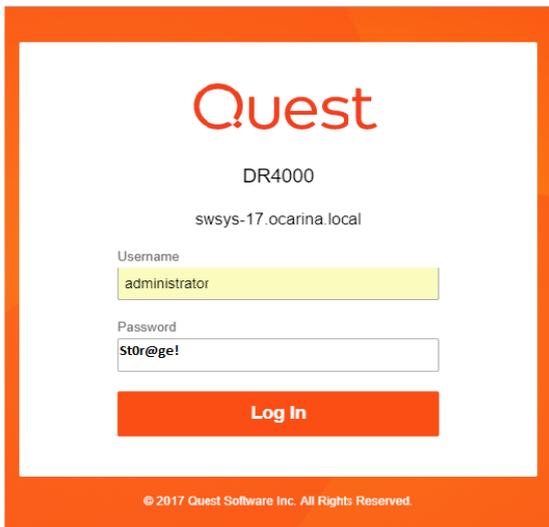


- 7 View the summary of preferences and confirm that it is correct.

```
=====
                          Set Static IP Address
IP Address                 : 10.10.86.100
Network Mask               : 255.255.255.128
Default Gateway           : 10.10.86.126
DNS Suffix                 : idmdemo.local
Primary DNS Server        : 10.10.86.101
Secondary DNS Server      : 143.166.216.237
Host Name                  : swsys-17

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

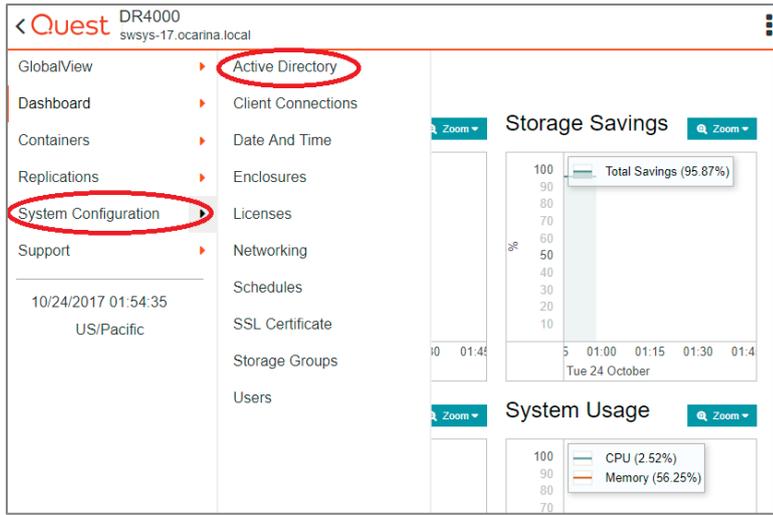
- 8 Log on to the DR Series system administrator console, using the IP address you just provided for the DR Series system and the username **administrator** and password **St0r@ge!** (the “0” in the password is the numeral zero).



- 9 Join the DR Series system to Active Directory.

i **NOTE:** If you do not want to add the DR Series system to Active Directory, see the *DR Series Deduplication Appliance Owner's Manual* for guest login instructions.

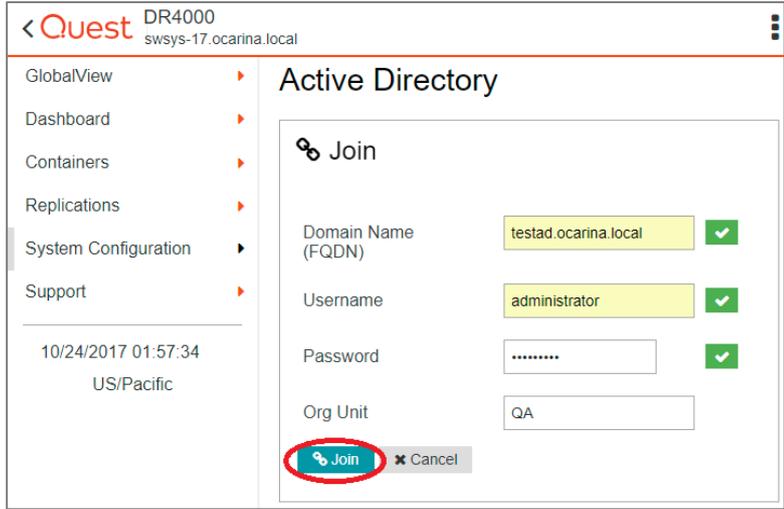
- a Select **Active Directory** in the left navigation area of the GUI.



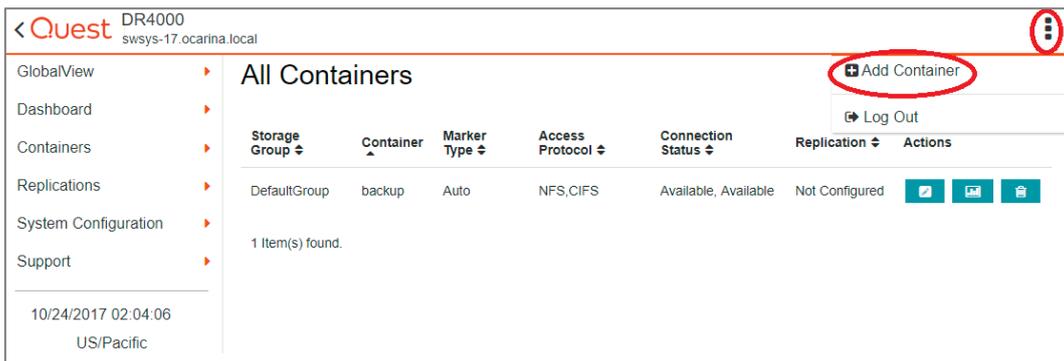
b Click **join** to enter your Active Directory credentials.



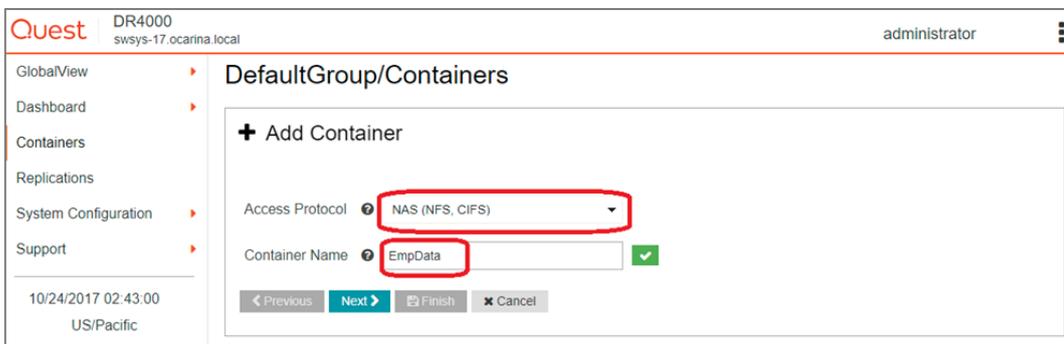
c Enter your Active Directory credentials.



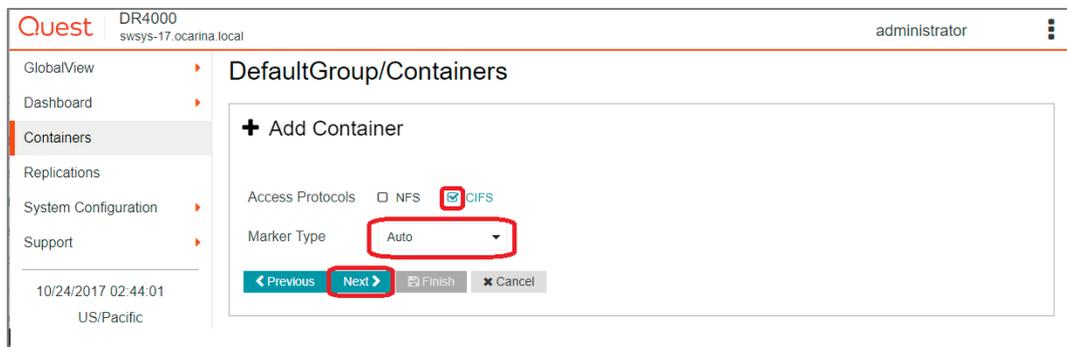
10 Create and mount the container as follows. Select **Containers** in the left navigation area of the DR Series system GUI, and then select the **Action Menu** in the upper right corner. Click the **Add Container** option at the top of the menu.



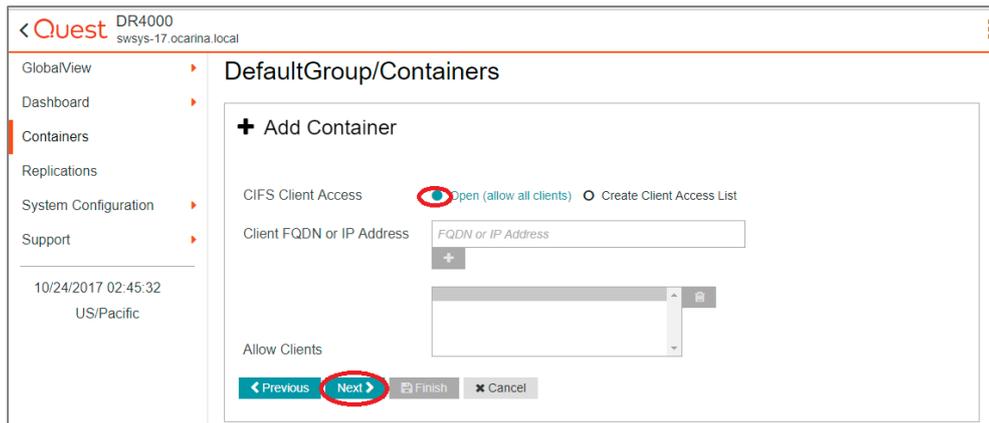
11 Choose the Access Protocol as 'NAS' (AppAssure supports CIFS protocols) and Enter a **Container Name** and then click **Next**.



a Enable **CIFS** checkbox, (AppAssure supports CIFS protocols) and then click **Next**.

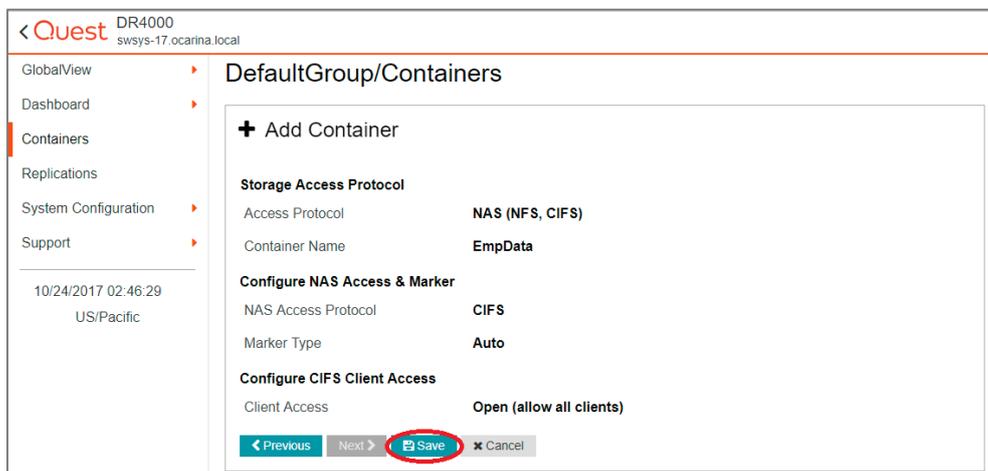


b Select the preferred client access credentials.

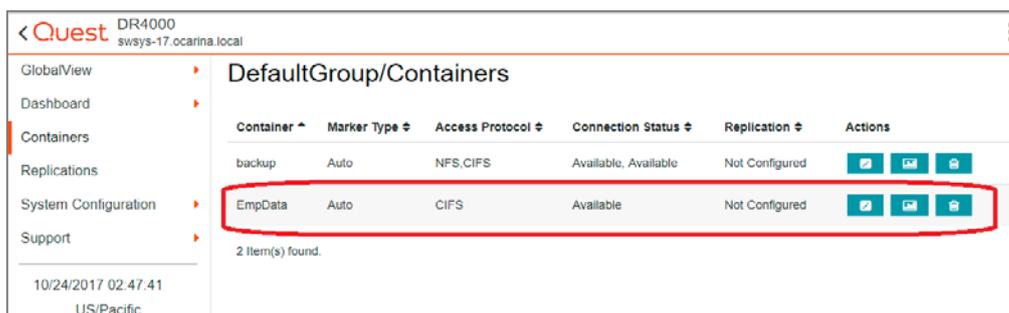


i **NOTE:** For improved security, Quest recommends adding IP addresses for the backup console (AppAssure Core, AppAssure Agent). Not all environments will have all components included.

12 Click **Save** to complete container creation.



13 Confirm that the container has been added.



14 Click the Statistics icon to get the container share/export path, which you will use later to target the DR Series system.

Quest DR4000
swsys-17.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

DefaultGroup/Containers

Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
backup	Auto	NFS,CIFS	Available, Available	Not Configured	[Icons]
EmpData	Auto	CIFS	Available	Not Configured	[Icons]

2 Item(s) found.

10/24/2017 02:47:41
US/Pacific

You will see the container stats and share/export path of the container as shown in the following example.

Quest DR4000
swsys-17.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

Active Files

Zoom

Files

Active Bytes

Zoom

Bytes

Throughput

Zoom

MB/s

Read
Write

Marker Type: Auto Connection Type: CIFS Total Files: 0

CIFS Connection Configuration

CIFS share path: **\swsys-17.ocarina.local\EmpData**

Client Access: Open Access (all clients have access)

CIFS Write Accelerator: inactive

10/24/2017 02:49:27
US/Pacific

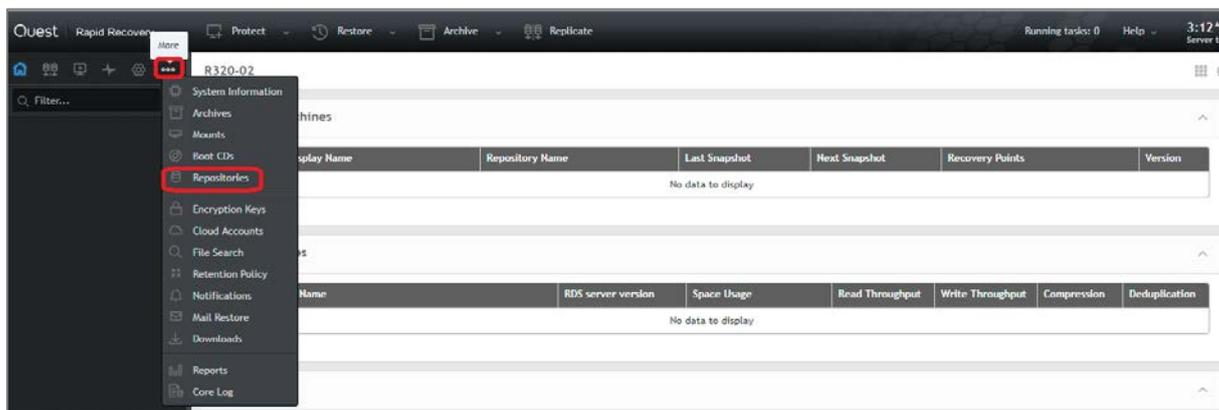
Setting up AppAssure

Archiving backup images to the DR Series system

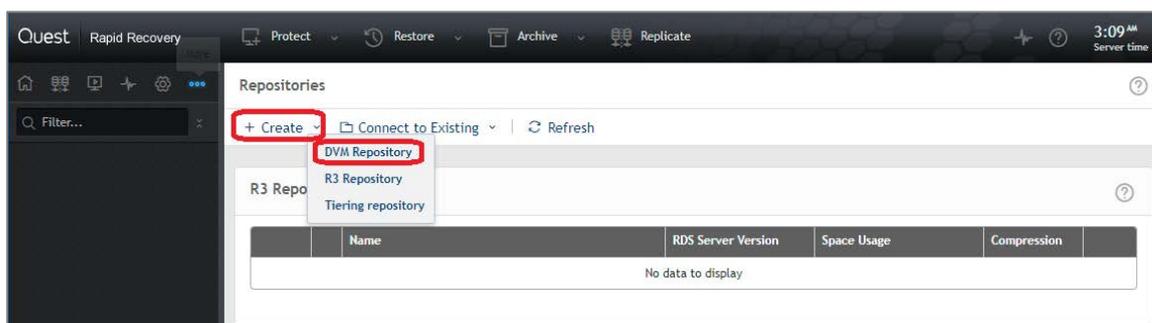
To create a backup job and back up a Windows data set, follow steps 1-10 in the procedure that follows. If you already have a backed up data set, skip steps 1-10 and start from step 11 to archive the backup data set to the DR Series system.

i **NOTE** *About Linux backup images:* Steps 9-12 in the following procedure are for archiving both Windows and Linux backup images. To generate Linux backup images, see *Installing the Linux agent*.

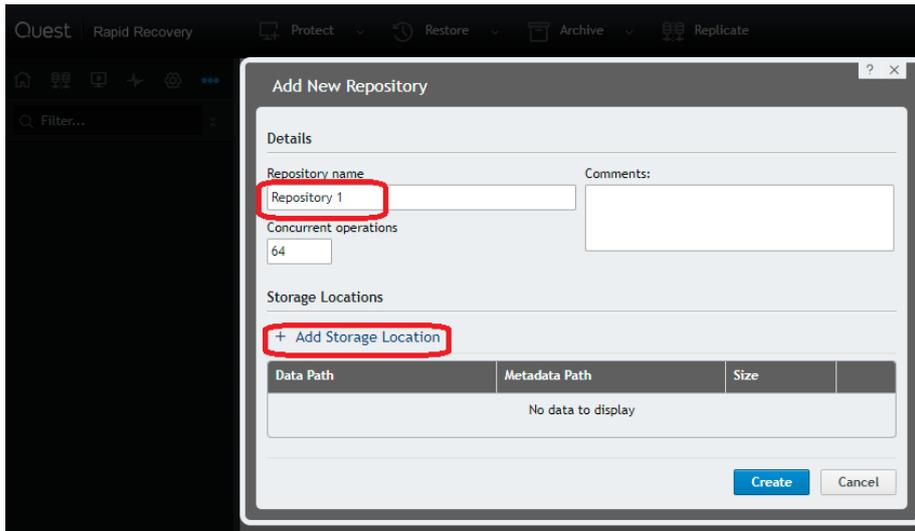
- 1 Log on to the AppAssure Core and click **Repositories**.



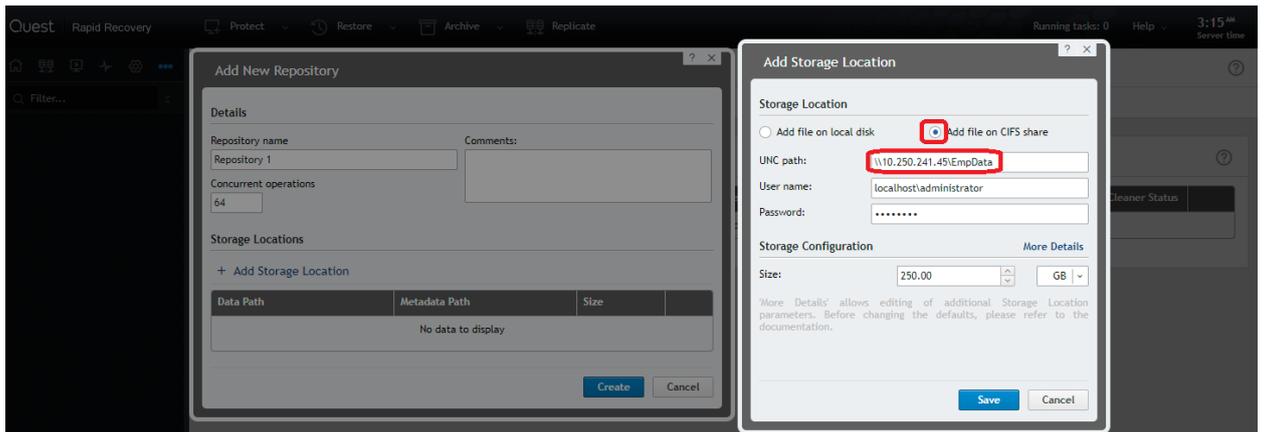
- 2 Click **Create > DVM Repository**.



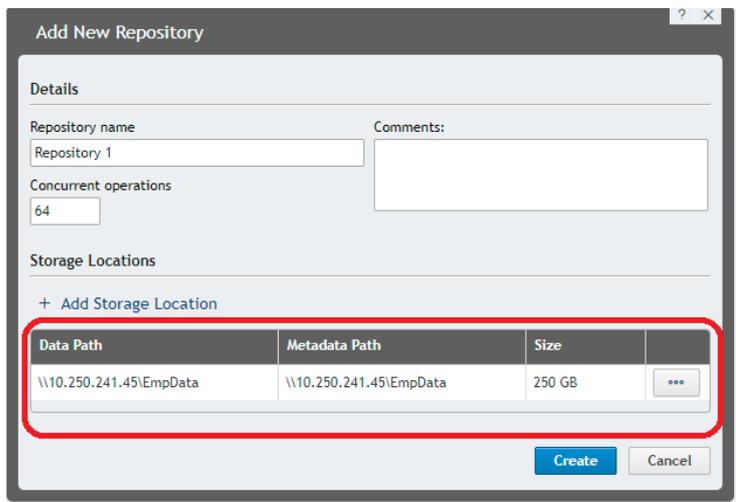
- 3 Type a repository name and click **Add Storage Location**.



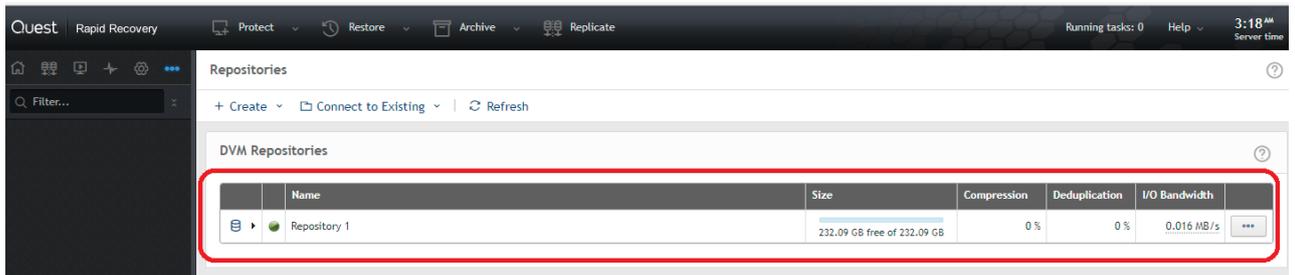
- 4 Enter the **Storage Location** details, and then click **Save**. The storage location is the target location for the backup job (DR container share/export shared location).



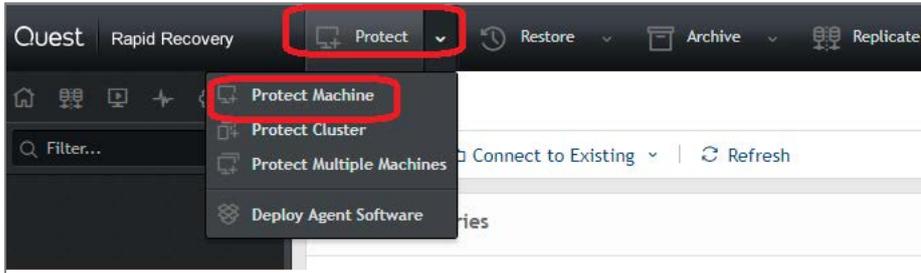
- 5 Click **Create**.



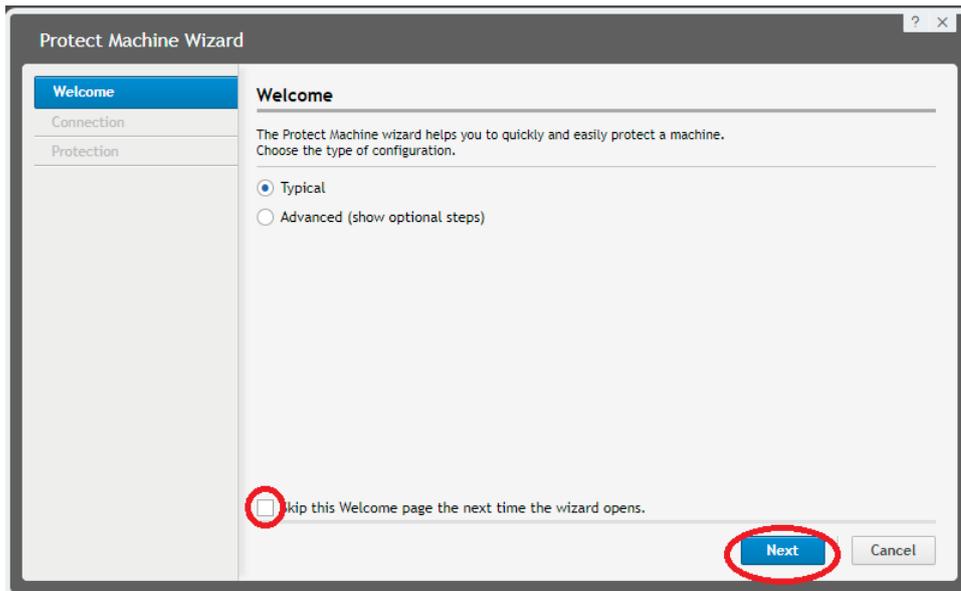
- 6 Verify the Repository has been created in the list of DVM repositories.



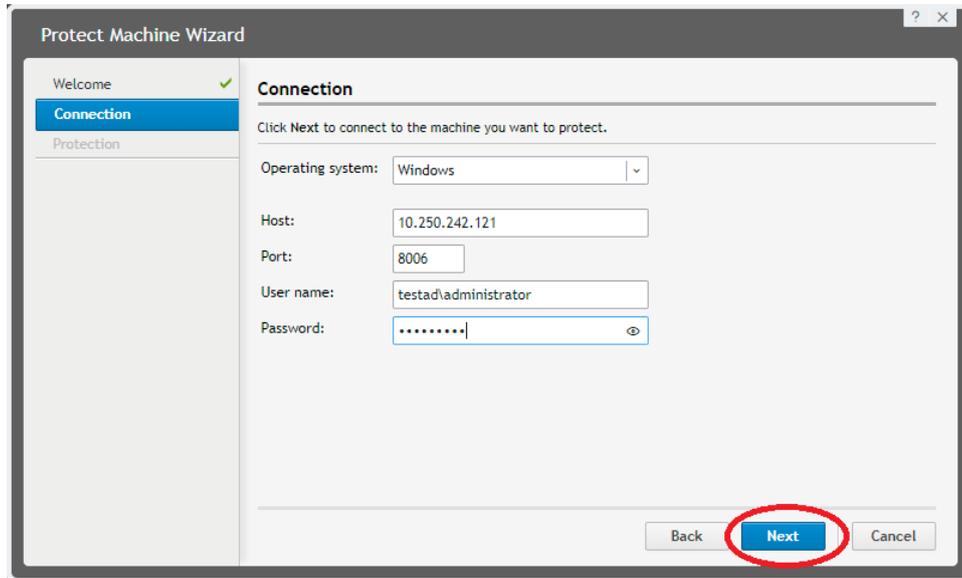
- 7 In the AppAssure core console, click **Protect > Protect Machine**.



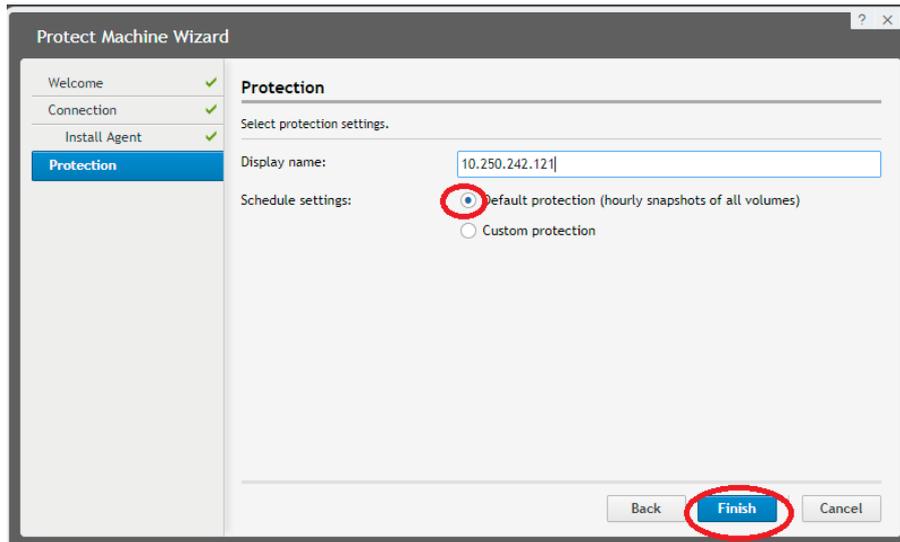
- 8 Select the type of configuration to protect as either **Typical** or **Advanced** and click **Next**.



- 9 If you selected Typical, do the following:
- a Enter the details for the protected/client machine and click **Next**.

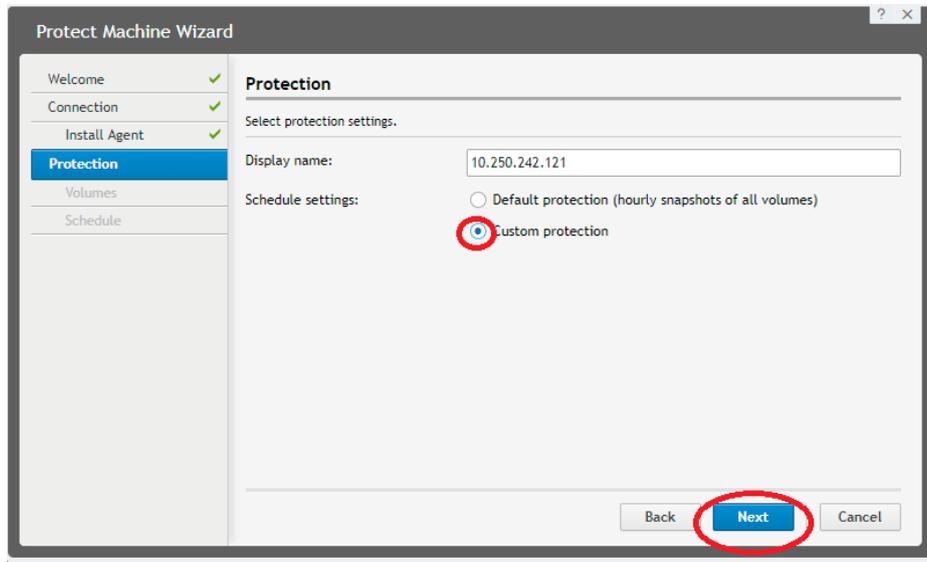


- b For default protection settings, select **Default Protection** and click **Finish**.

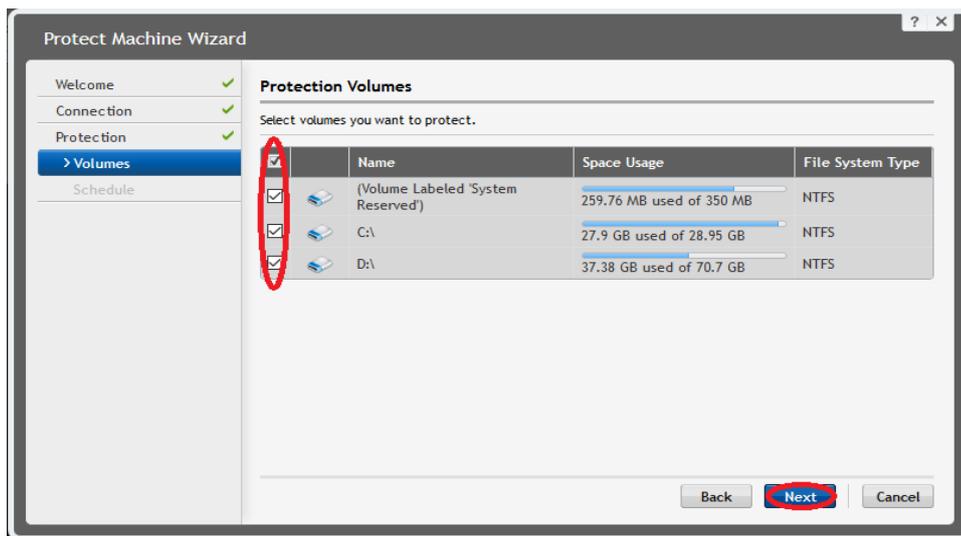


c For Custom protection settings, do the following.

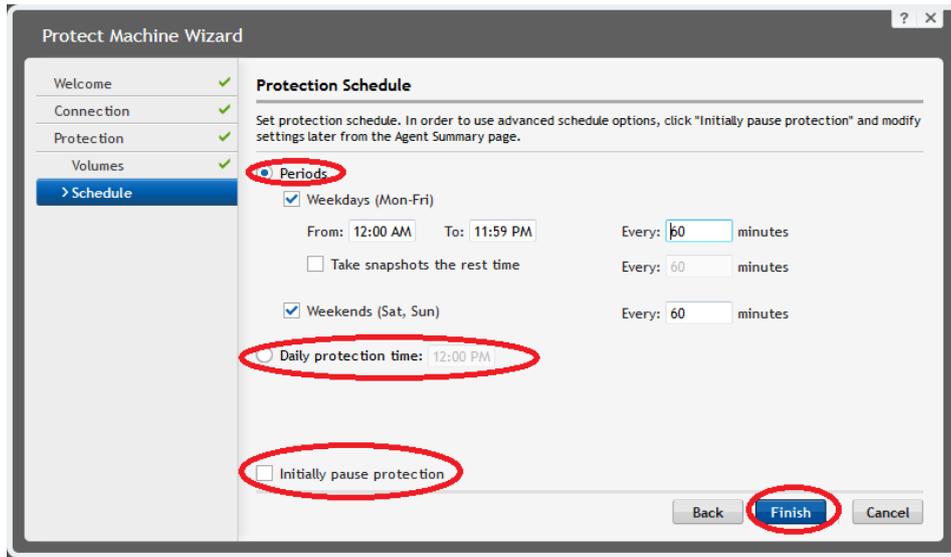
a Select Custom Protection and click **Next**.



b Select the volumes to protect and click **Next**.

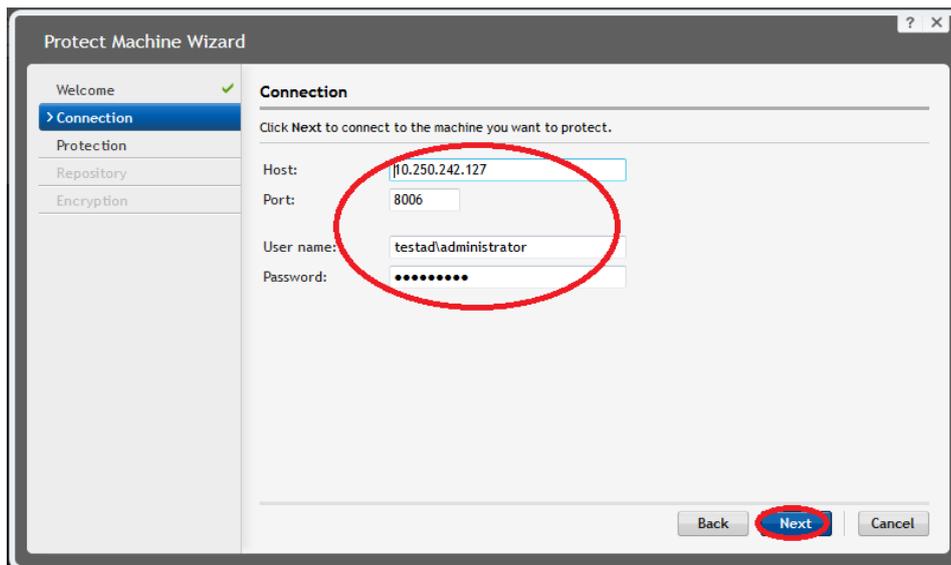


- c Select the protection schedule and click **Finish**.

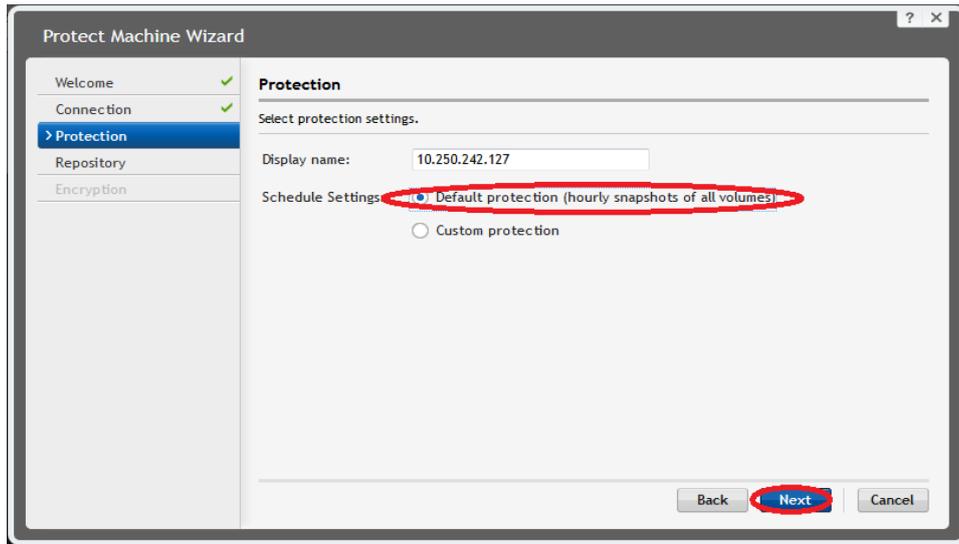


- 10 If you selected the Advanced configuration type, do the following:

- a Enter the details for the protected machine/client machine and click **Next**.

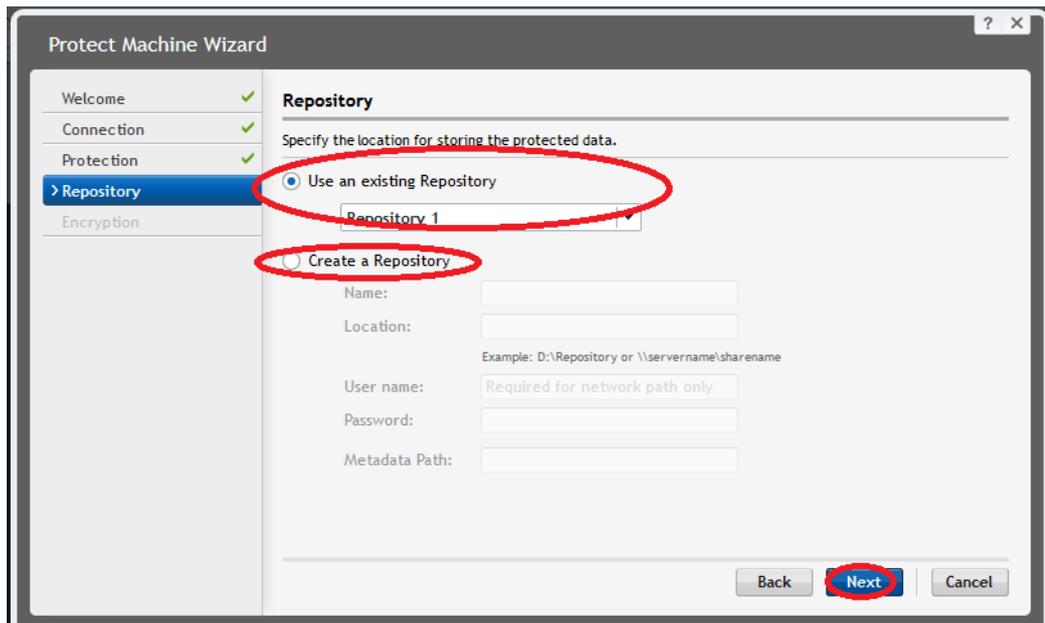


- b Select the **Default Protection** option and click **Next**.

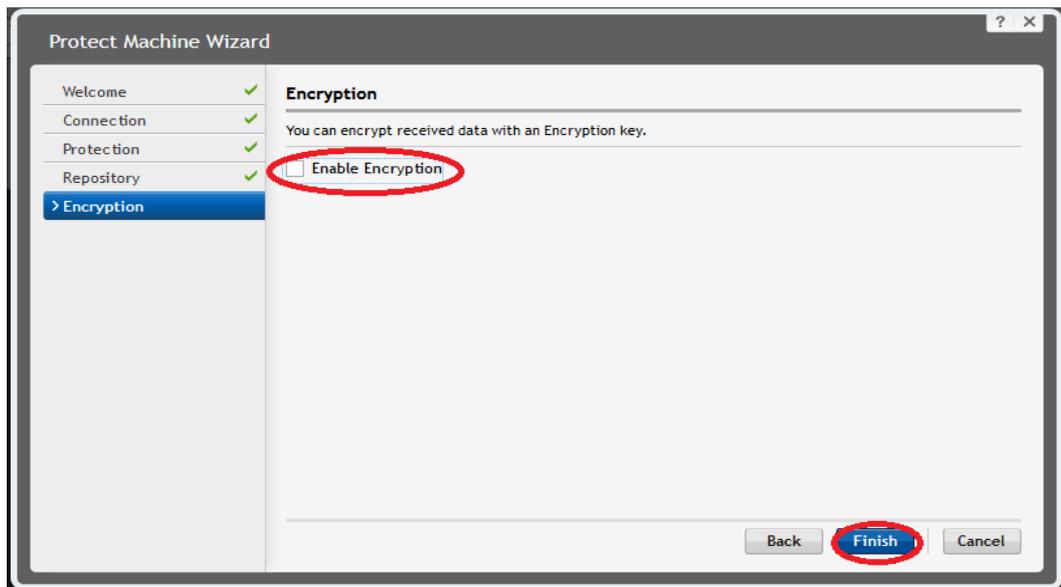


- c Select one of the following options for the location for storing protected data and click **Save**:

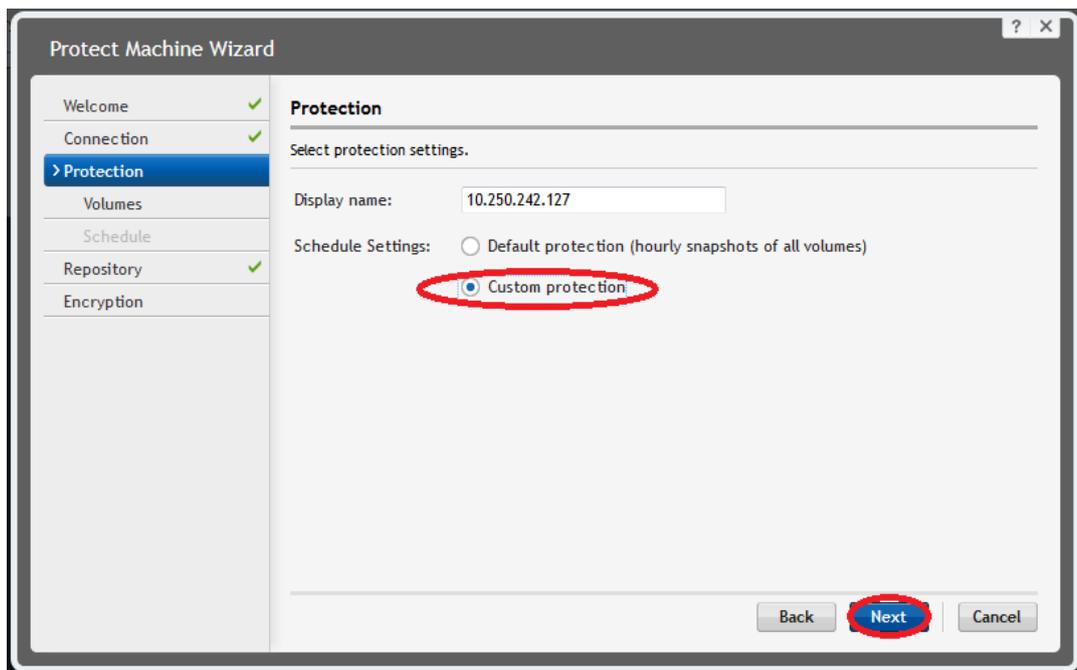
- Use an existing repository** - To select an existing repository.
- Create new repository** – To create a new repository.



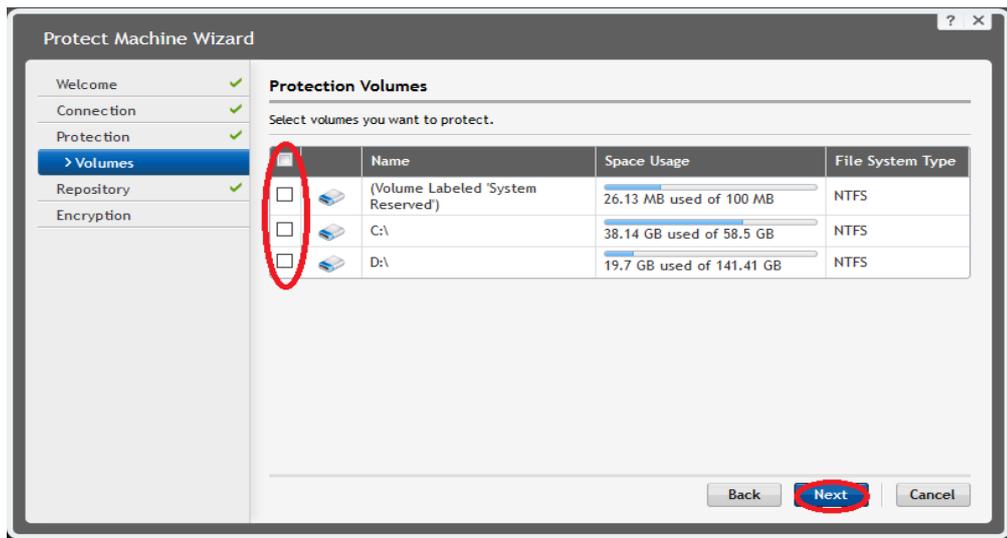
- d To encrypt data during protection, select **Enable Encryption** and click **Finish**; otherwise, click **Finish**.



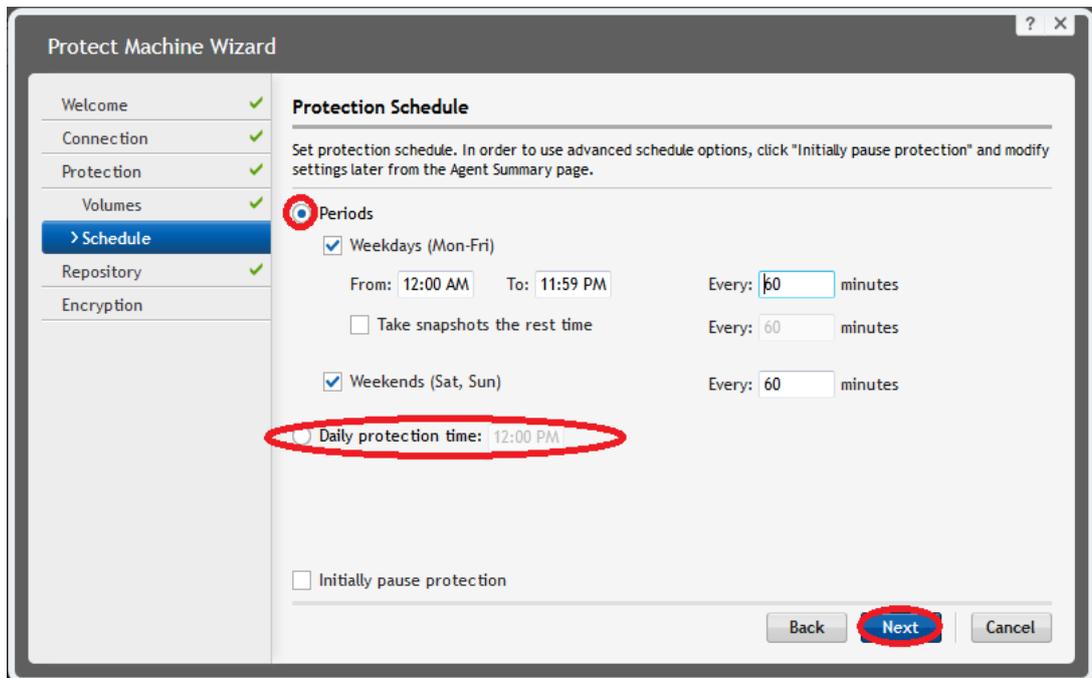
- e Select the **Custom Protection** option and click **Next**.



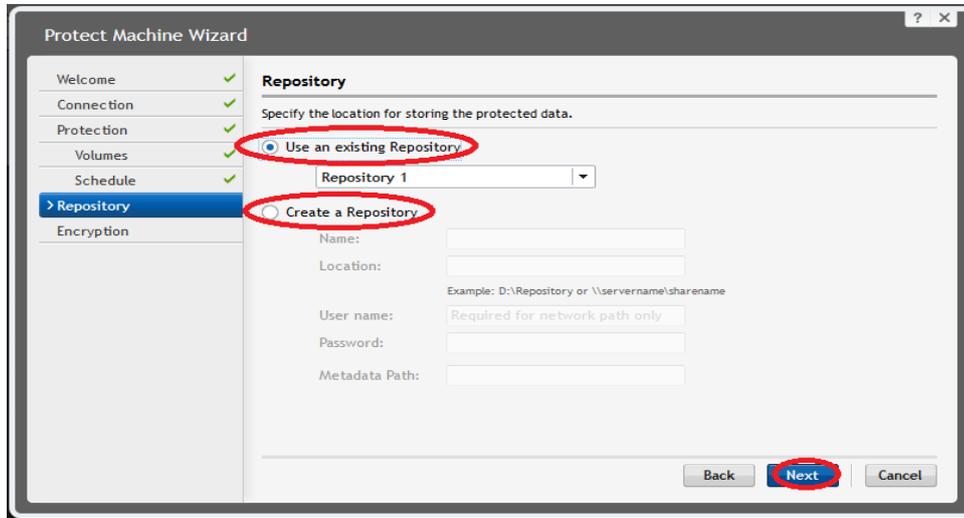
- f Select the volumes to protect and click **Next**.



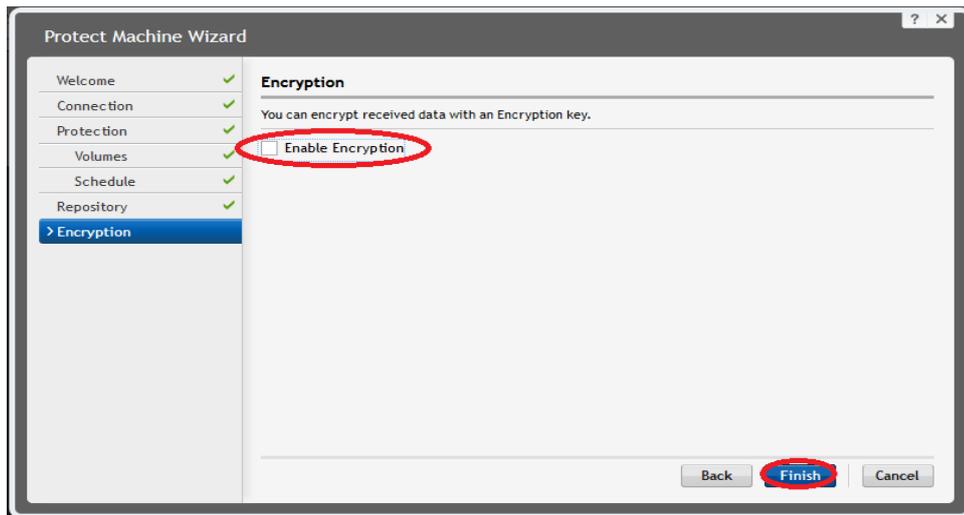
- g Select the appropriate protection schedule and click **Next**.



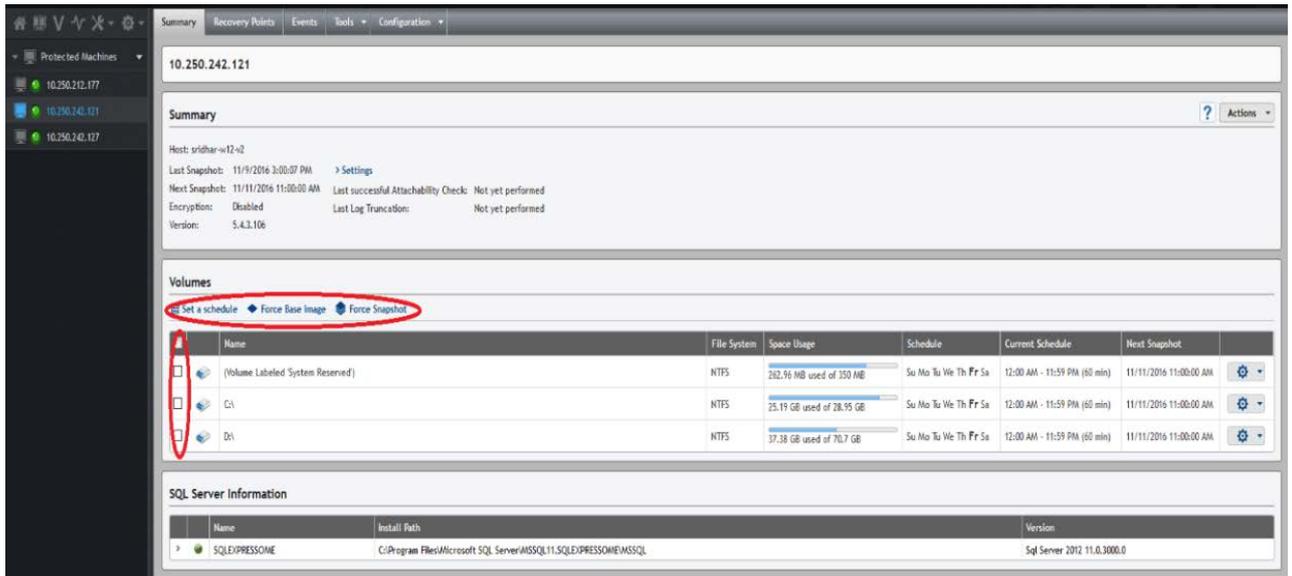
- h Select one of the following options for the location for storing protected data and click **Save**:
- Use an existing repository** - To select an existing repository.
 - Create new repository** – To create a new repository.



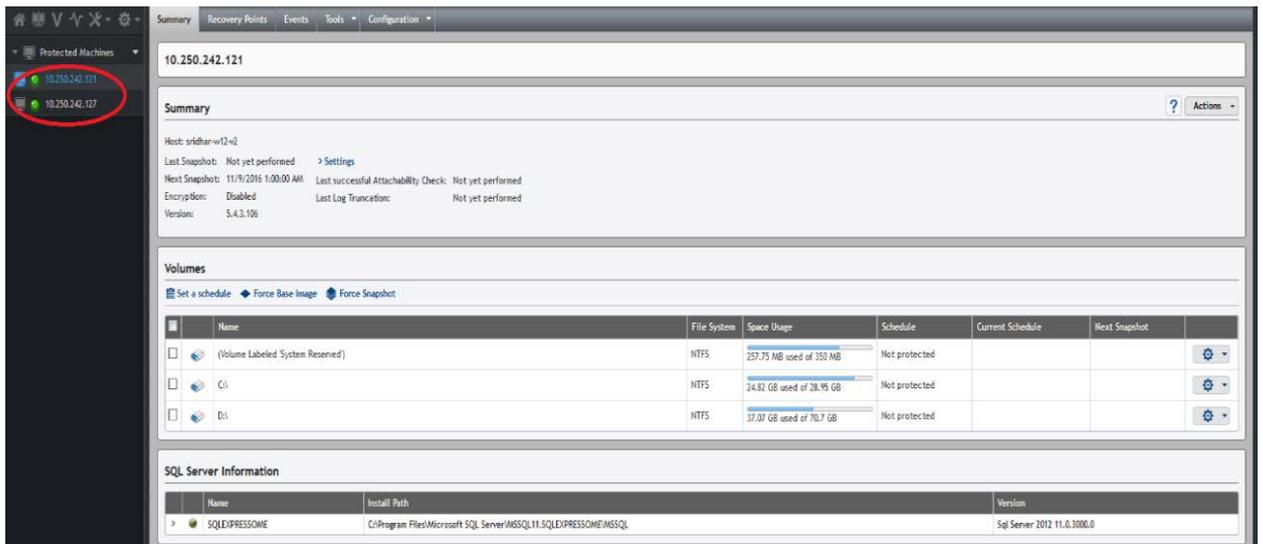
- i If you want to encrypt the data during the protection, select **Enable Encryption** and click **Finish**; otherwise, click **Finish**.



- 11 Select or clear the checkbox next to each volume group to select the backup data set. To change backup schedules, click **Set a Schedule**.

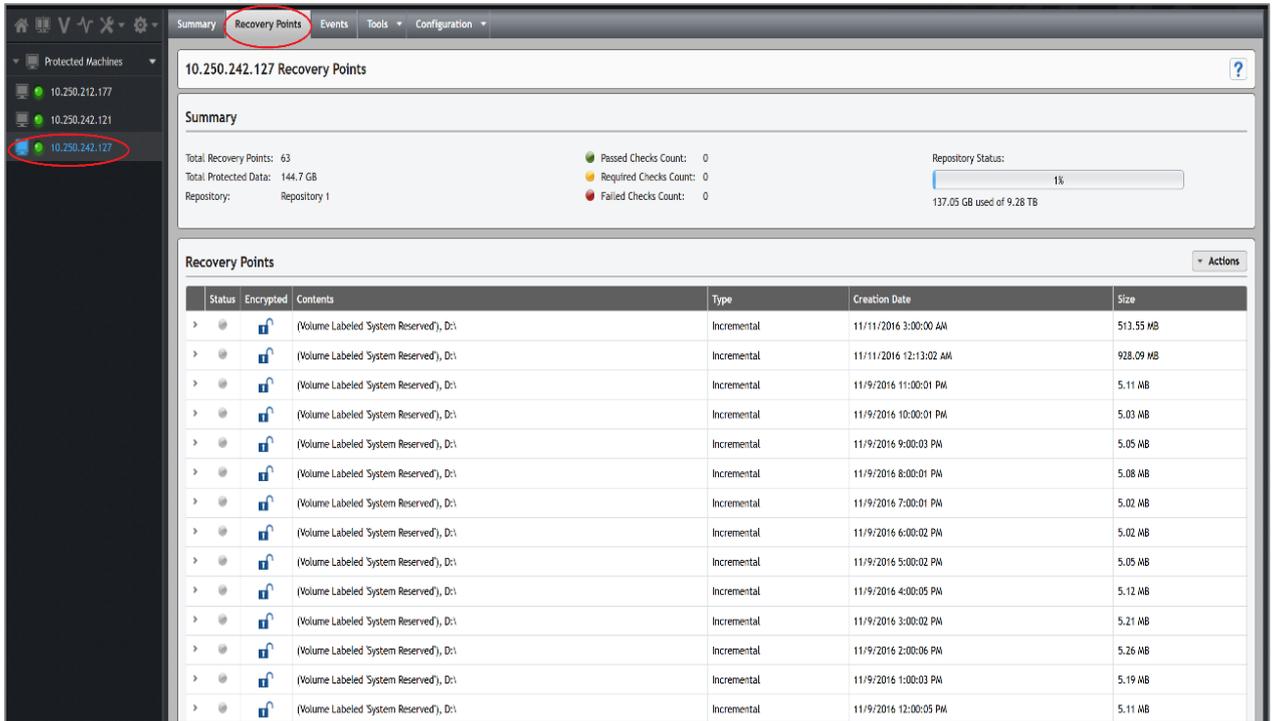


The machines that have been protected by AppAssure are listed on the left side under **Protected Machines**.

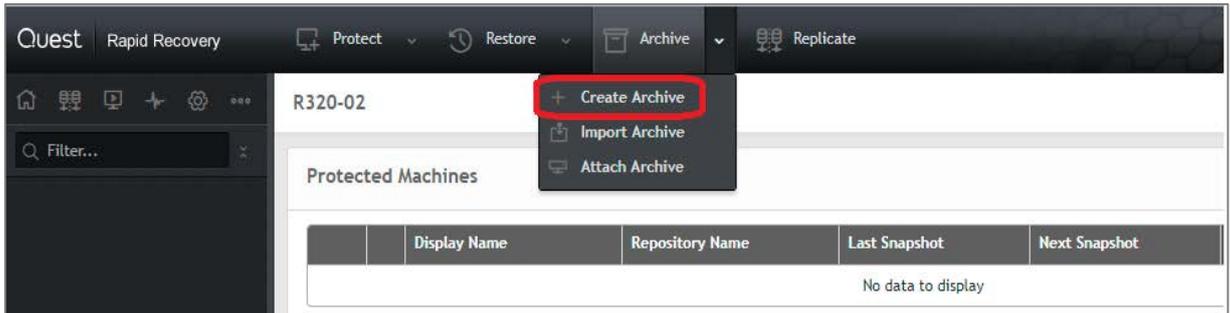


AppAssure creates backup images for the protected machines according to the protection policy.

12 To see the backup images, click **Protected Machines > Recovery Points**.



13 To create an archive job, click **Archive > Create Archive**.



14 Enter all of the required archive location information and then click **Next**.

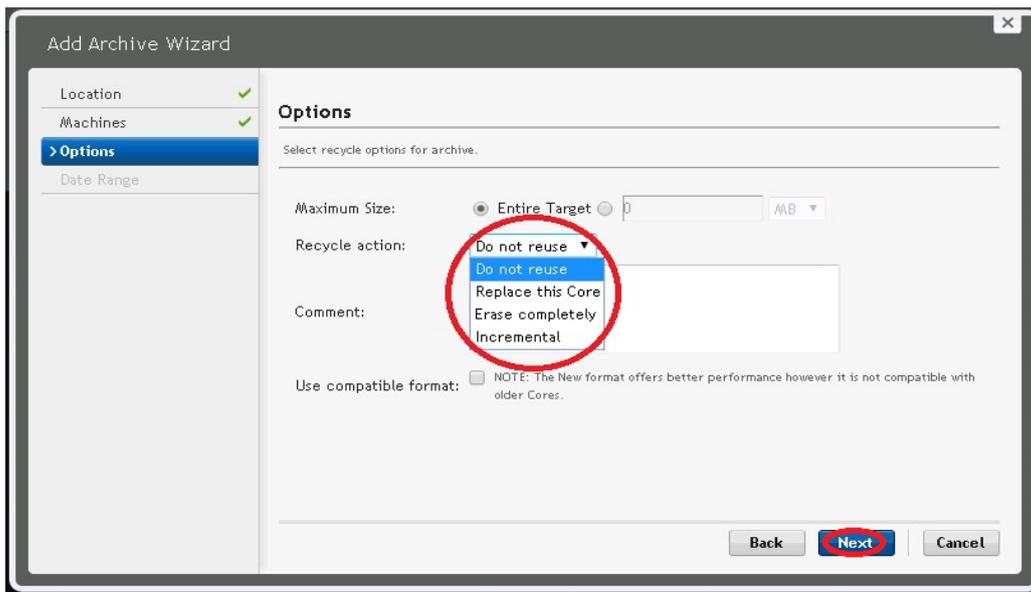
The screenshot shows the 'Archive Wizard' dialog box. On the left, a sidebar contains 'Archive Type' (checked), 'Location' (selected), 'Machines', and 'Options'. The main area is titled 'Location' and contains the instruction 'Select the location where you want to save the archive.' Below this are four input fields: 'Location type' (set to 'Network'), 'Location' (set to '\\swsys-17.testad\EmpData' with a subtext 'Example network path: \\servername\sharename'), 'User name' (set to 'testad\administrator'), and 'Password' (masked with dots). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

15 Select the machines that you want to archive and click **Next**.

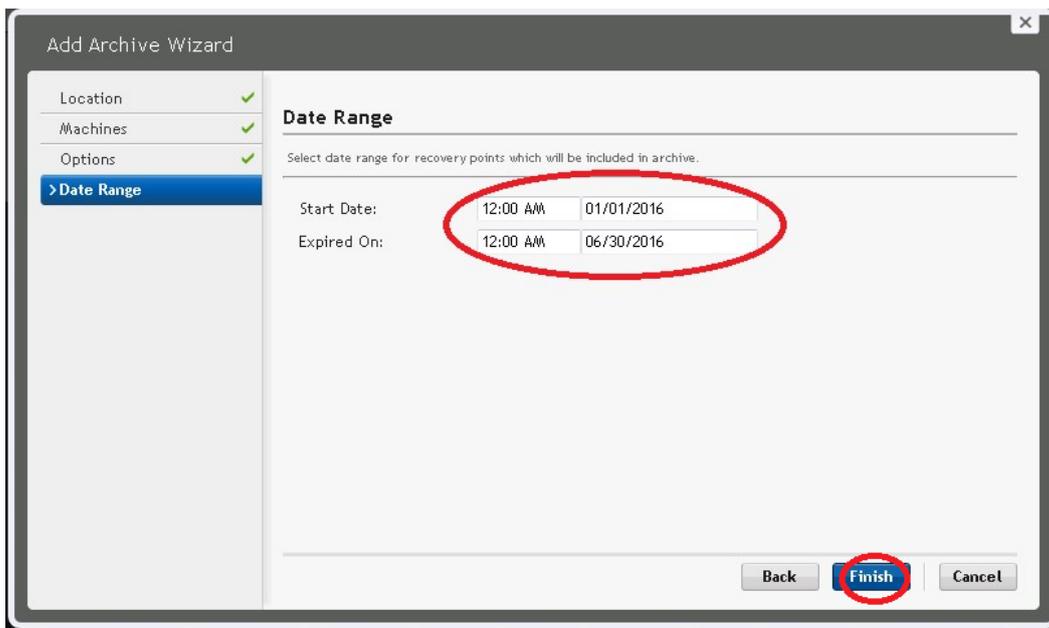
The screenshot shows the 'Add Archive Wizard' dialog box. On the left, a sidebar contains 'Location' (checked), '> Machines' (selected), 'Options', and 'Date Range'. The main area is titled 'Machines' and contains the instruction 'Select the protected machines that you want to archive.' Below this is a table with three columns: a checkbox, 'Display Name', and 'Recovery Points'. The table lists two machines. A red circle highlights the first checkbox, and another red circle highlights the 'Next' button at the bottom right.

<input type="checkbox"/>	Display Name	Recovery Points
<input type="checkbox"/>	10.250.242.121	11
<input type="checkbox"/>	10.250.242.127	61

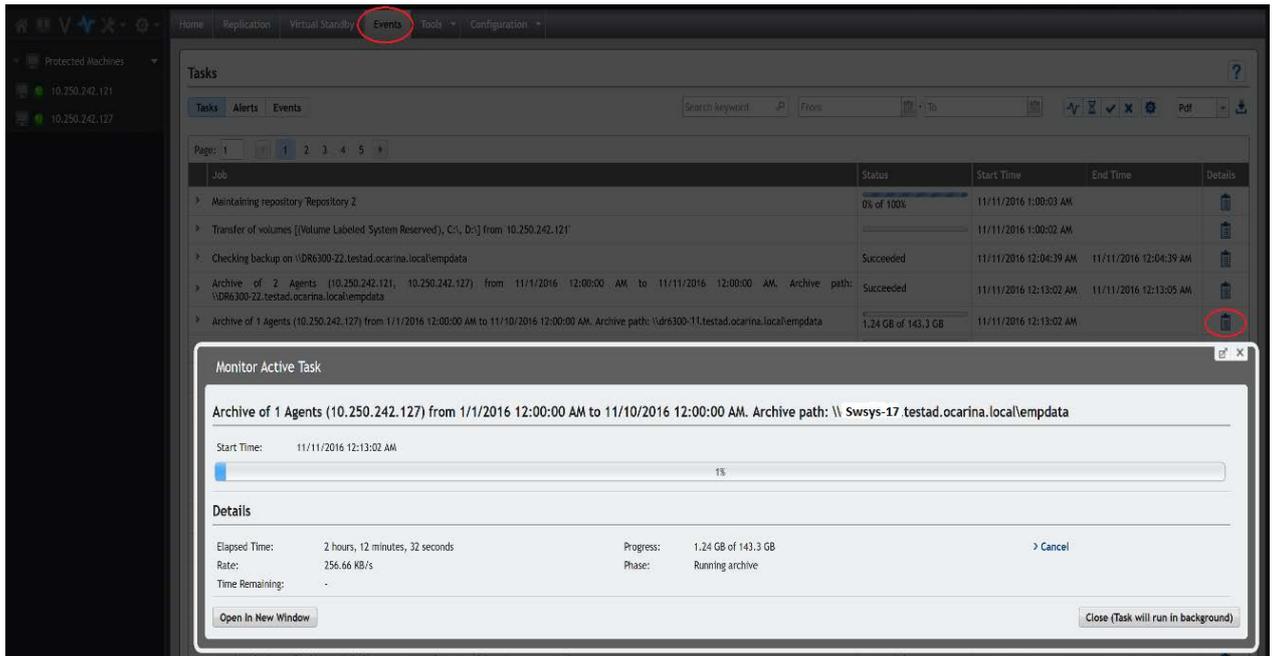
16 Select the required Recycle option to Archive and click **Next**.



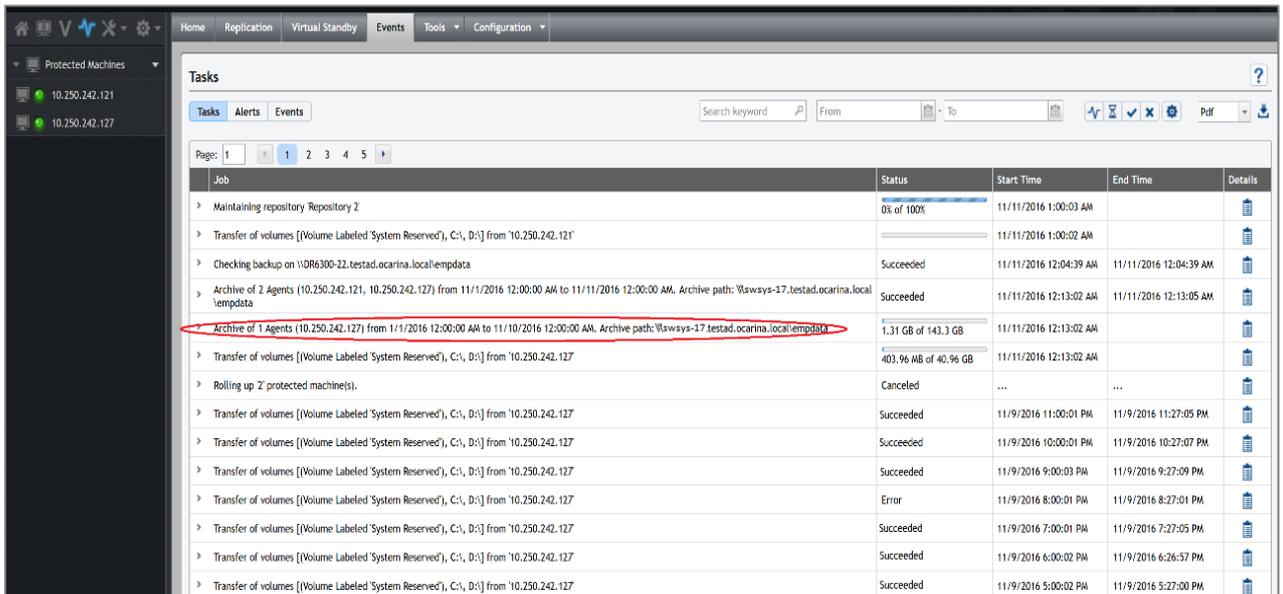
17 Select a date range for the recovery points and click **Finish**.



18 To check the archive job details, click the **Events** tab.



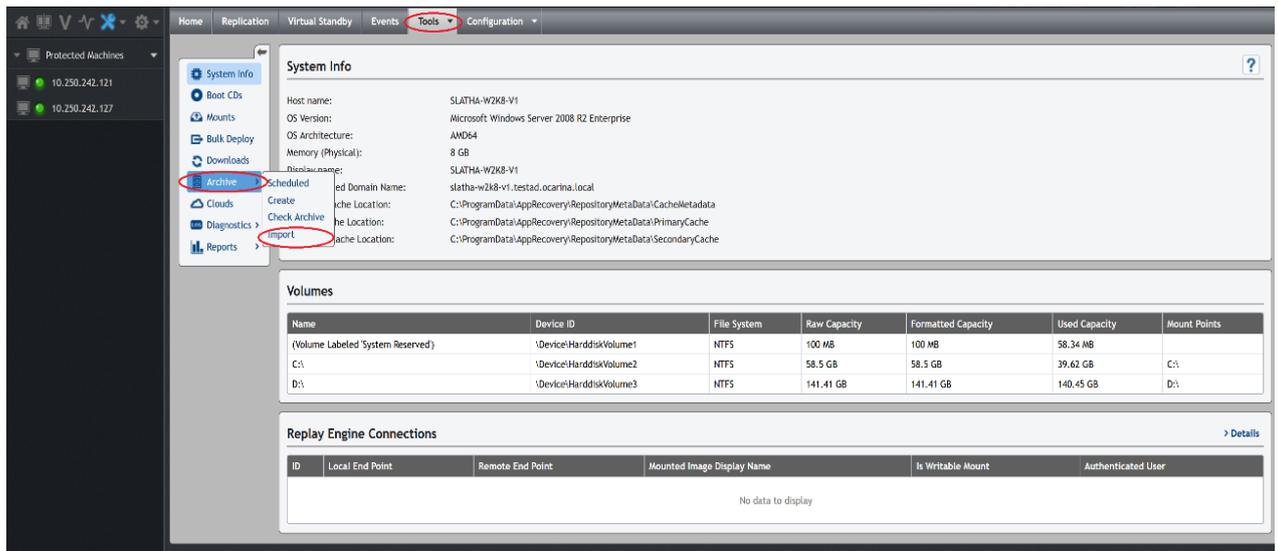
The archive job details are displayed on the **Events** tab.



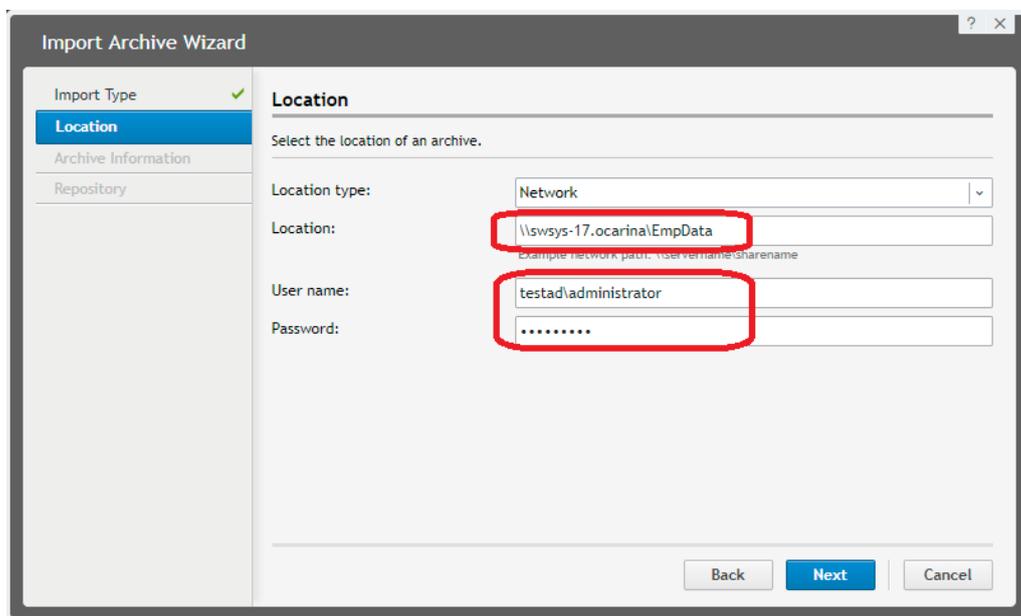
Restoring archived backup images from the DR Series system

Follow these steps to restore archived backup images from the DR Series system.

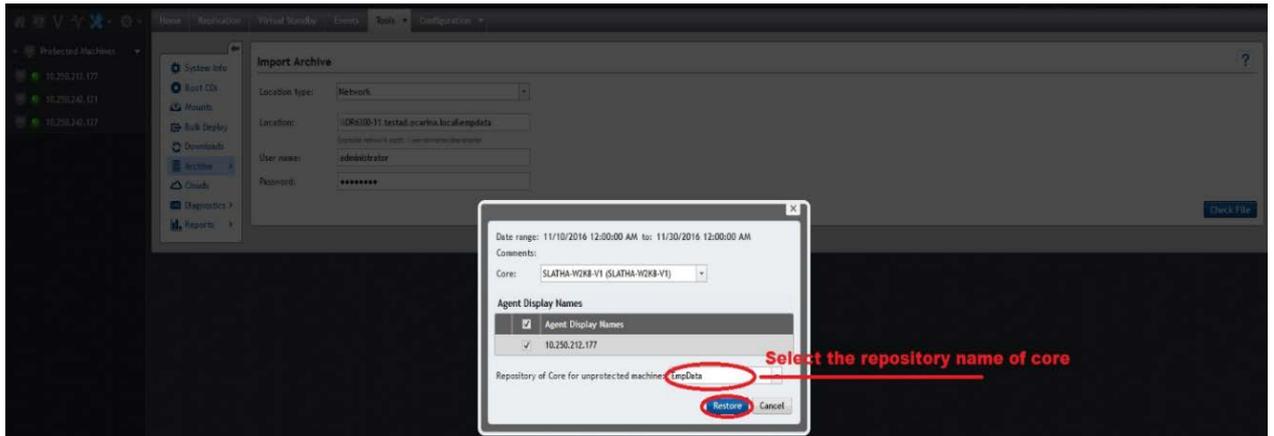
- 1 Click **Tools > Archive > Import**.



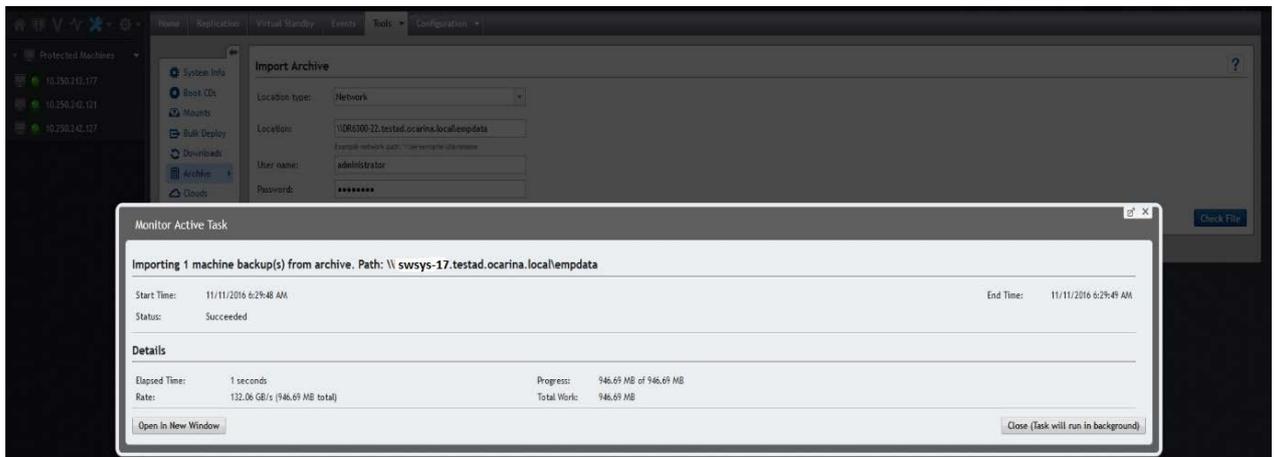
- 2 Enter the UNC path of the DR container share that holds the archive images. In addition, enter the CIFS credentials for authenticating to the DR Series system. Click **Check File**.



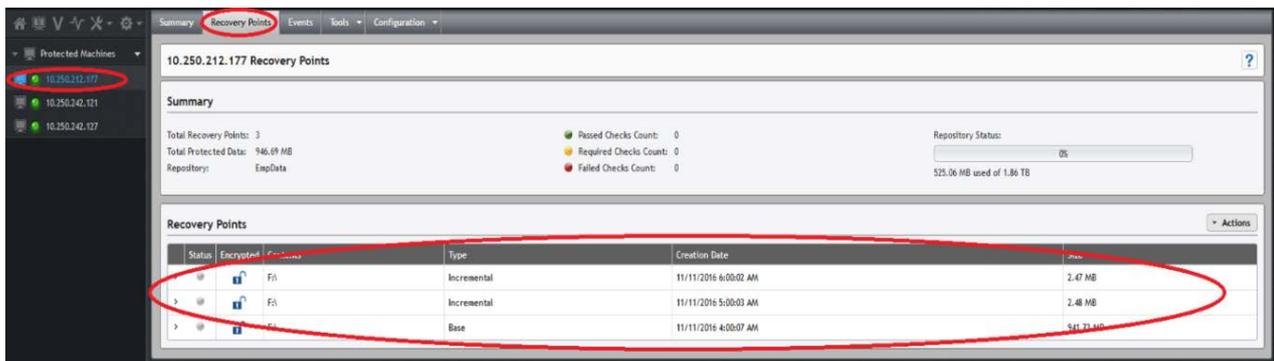
- 3 Under **Agent Names**, select the agent and repository that the archived data will be imported to and click **Restore**.



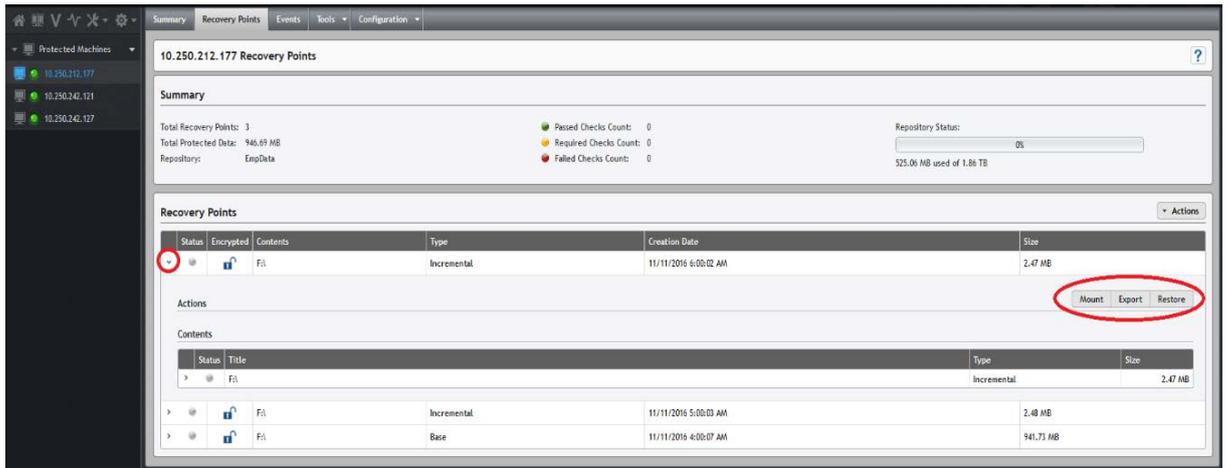
4 To monitor the restore process, click **Open Monitor Window**.



5 After the restore is completed, click **Protected Machines -> Recovery Points**. Verify that the recovery point(s) have been restored back to the repository.



6 You can expand the recovery points to view available operations.

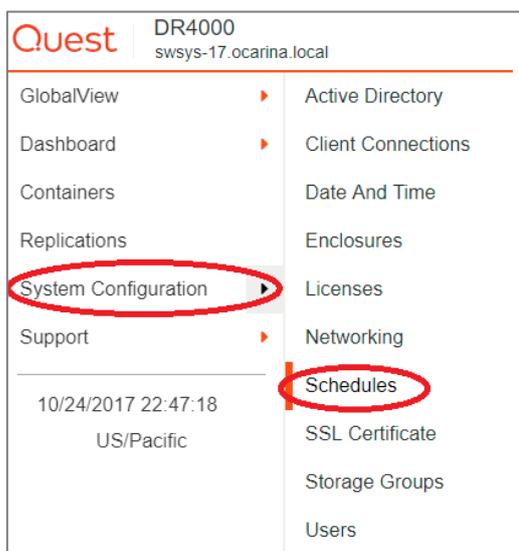


Setting up the DR Series system cleaner

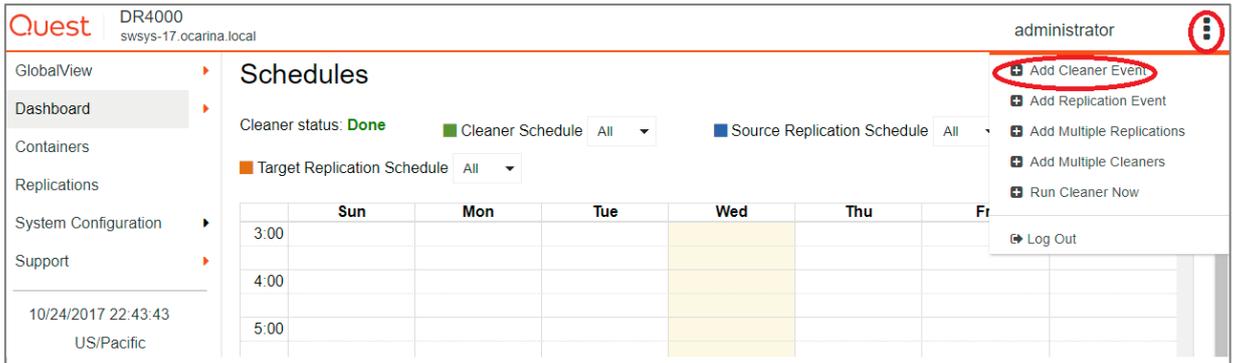
Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication. The cleaner runs during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner to force it to run during a scheduled time.

If necessary, you can perform the procedure described below to force the cleaner to run. After all of the backup jobs are set up, 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, and generally after a backup job has completed.

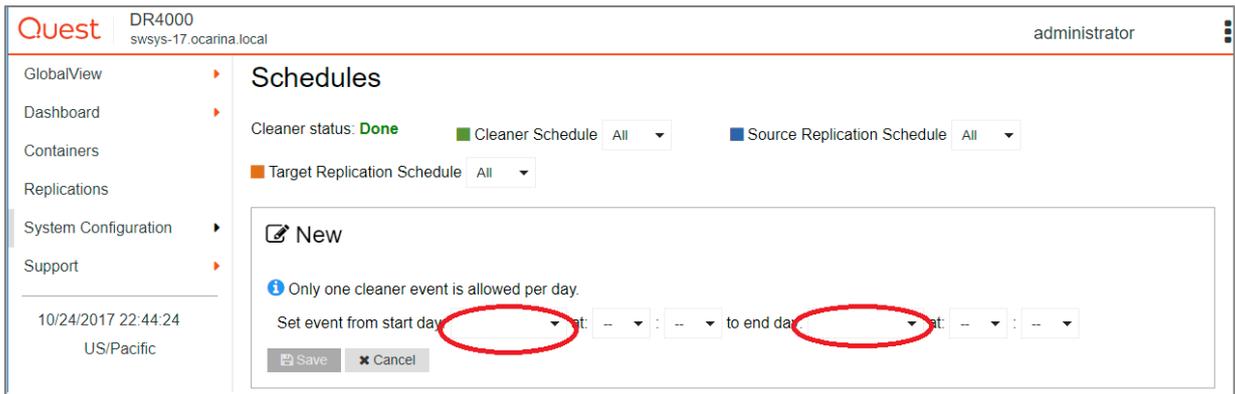
- 1 Click **System Configuration > Schedules**.



- 2 In the Action menu in the upper right part of the Schedules page, click **Add Cleaner Event**.



3 Set the schedule for the cleaner to run and click **Save**.

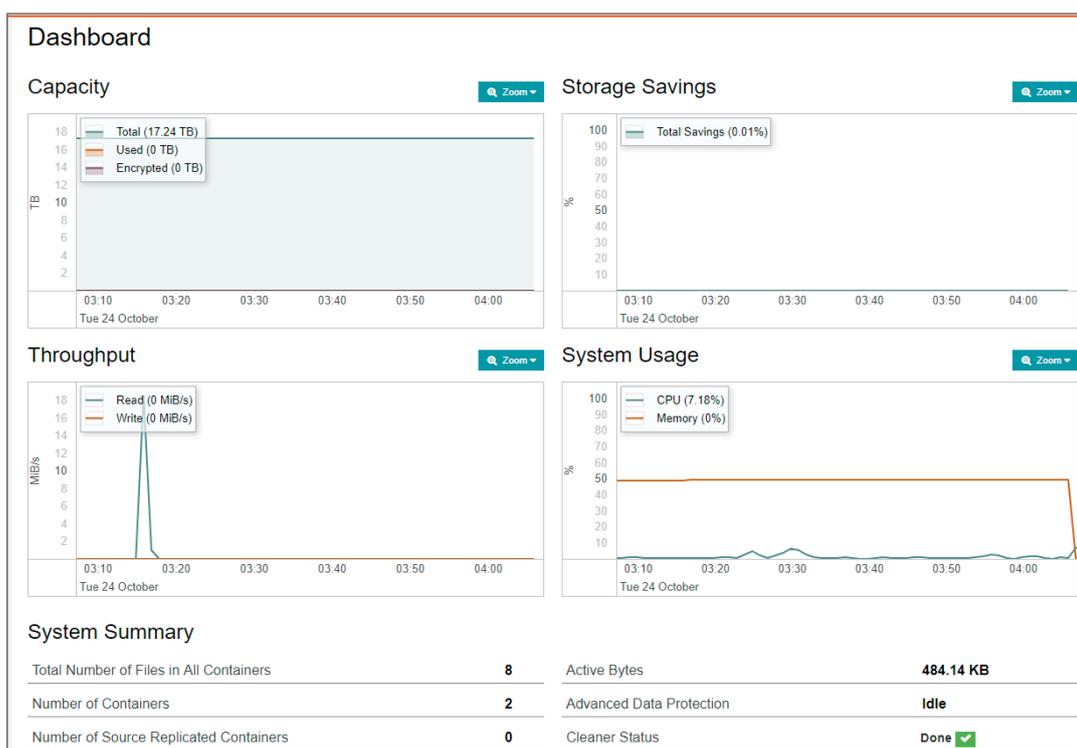


For additional guidance on setting up the system cleaner, refer to the white paper, *DR Series Cleaner Best Practices*. You can download this document from the [DR Series support site](#) by selecting your specific DR Series system model, and then navigating to the Technical Documentation page.

Monitoring deduplication, compression, and performance

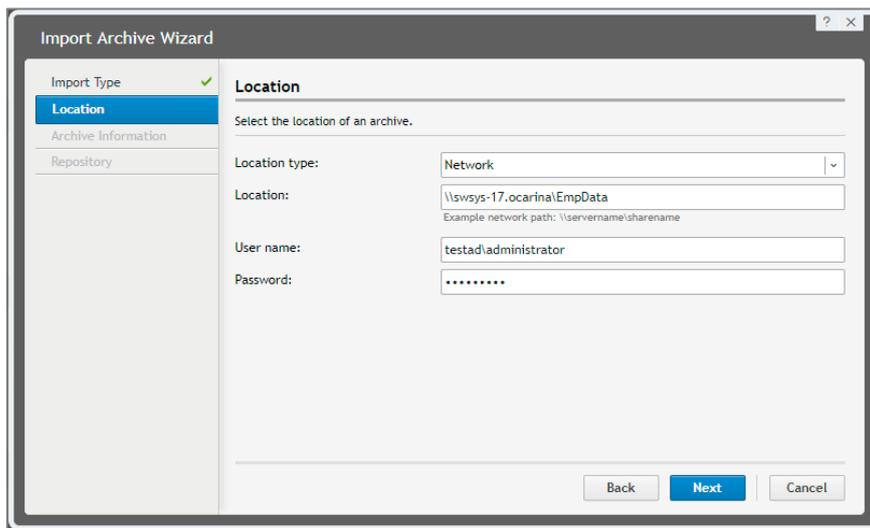
After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits of the DR Series system.

i **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 are completed, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio, in most cases.

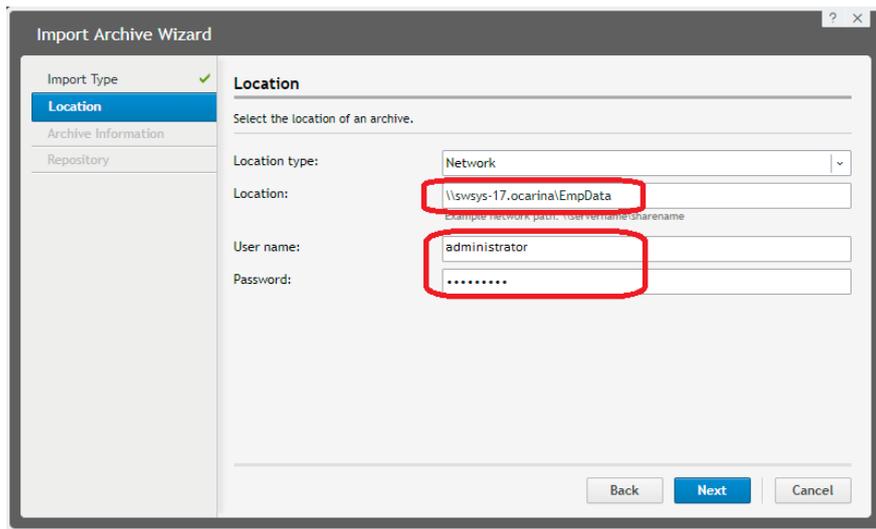


A - Configuring the DR container share as a CIFS storage device

To configure the DR container share as an archive destination, AppAssure needs to authenticate to a DR Series system. If the DR Series system is joined into an Active Directory domain, you must enter **[domain_name]user_id** in the User Name field for successful authentication.



NOTE: If the DR is configured as a standalone CIFS server, a DR local CIFS user credential can be used.



B - Backing up a Linux client

Installing the Linux agent

On the Linux client machine, run the commands below as the root user to install the Linux agent.

i | **NOTE:** For more details, see the *AppAssure User Guide*.

- 1 Create a new user for Linux Agent:

```
useradd approot
```

- 2 Set a password for the new user:

```
passwd approot
```

- 3 Add the user to the root, daemon, adm, and wheel groups.

```
usermod -G root,daemon,adm,wheel approot
```

```
root@IvanW-RHEL6-02:~/Downloads
File Edit View Search Terminal Help
[root@IvanW-RHEL6-02 Downloads]# useradd approot
[root@IvanW-RHEL6-02 Downloads]# passwd approot
Changing password for user approot.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@IvanW-RHEL6-02 Downloads]# usermod -G root,daemon,adm,wheel approot
[root@IvanW-RHEL6-02 Downloads]# groups approot
approot : approot root daemon adm wheel
[root@IvanW-RHEL6-02 Downloads]#
```

- 4 Install the Linux agent installer.

```
./appassure-installer_rhel_amd64_6.2.125.sh
```

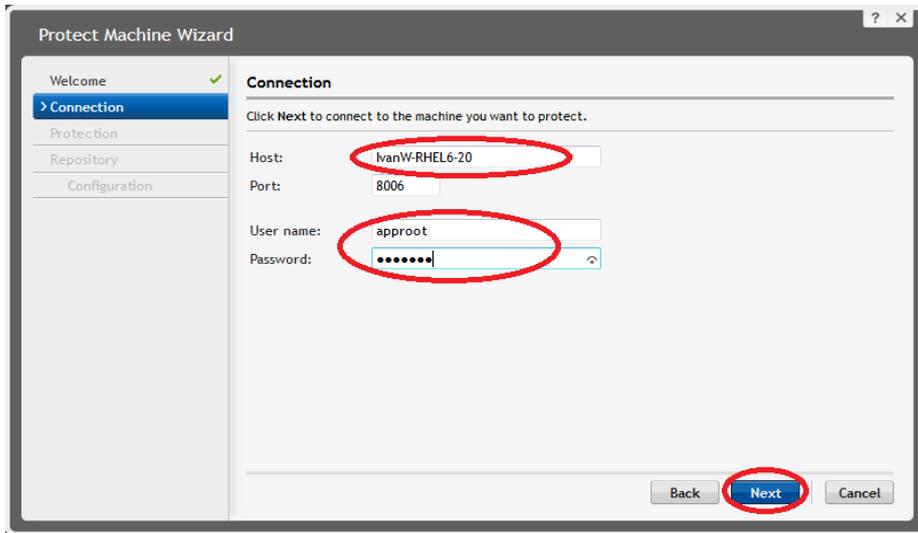
```
root@IvanW-RHEL6-02:~/Downloads
File Edit View Search Terminal Help
tar: appassure-packages/appassure-agent-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:45:17 is 1149951.791499555 s in the future
tar: appassure-packages/version: time stamp 2013-11-03 16:46:03 is 1149997.790834578 s in the future
tar: appassure-packages/appassure-vss-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:46:03 is 1149997.787838757 s in the future
tar: appassure-packages/appassure-mono-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:46:02 is 1149995.26755657 s in the future
tar: appassure-packages/appassure-vdisk-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:45:12 is 1149945.264826559 s in the future
tar: appassure-packages/mbd-dkms-2.6.32.el6.noarch.rpm: time stamp 2013-11-03 16:47:51 is 1150104.264341006 s in the future
tar: appassure-packages: time stamp 2013-11-03 16:47:51 is 1150104.263594253 s in the future
Configure default port for Agent [8006]:
AppAssure Agent will listen on port 8006
Now add some users to group 'appassure' to grant them permission to protect the machine
Enter a list of users allowed to protect the machine (ex: jsmith,ajohnson) [none]
aproot
A reboot is required to apply installation changes
Would you like to reboot after installation? [Y/n] y
```

i | **NOTE:** You can download the Linux agent installer from the AppAssure 5.x link here: <http://docs.appassure.com/display/AA50D/AppAssure+5+Previous+Builds>.

Configuring the Linux client machine

Follow these steps to configure the Linux client machine.

- 1 On the AppAssure Core Console, click **Protect -> Protect Machine**.
- 2 In the Connect dialog box, enter the information about the client machine, and then click **Next**.



i | **NOTE:** Use the **aproot** user, which was added during agent installation.