

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

## Technical White Paper

Quest Engineering

October 2017



## 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.

# Contents

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

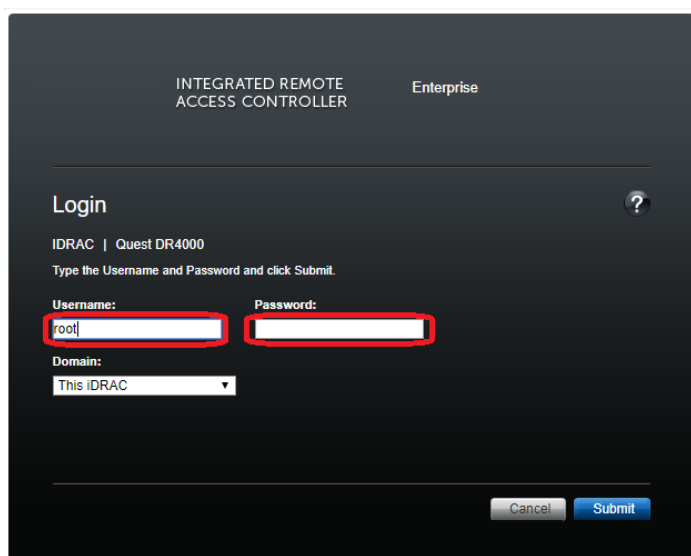


**NOTE:** The DR Series system/ AppAssure build version and screenshots used in this document may vary slightly, depending on the version of the DR Series system/ AppAssure Software version you are using.

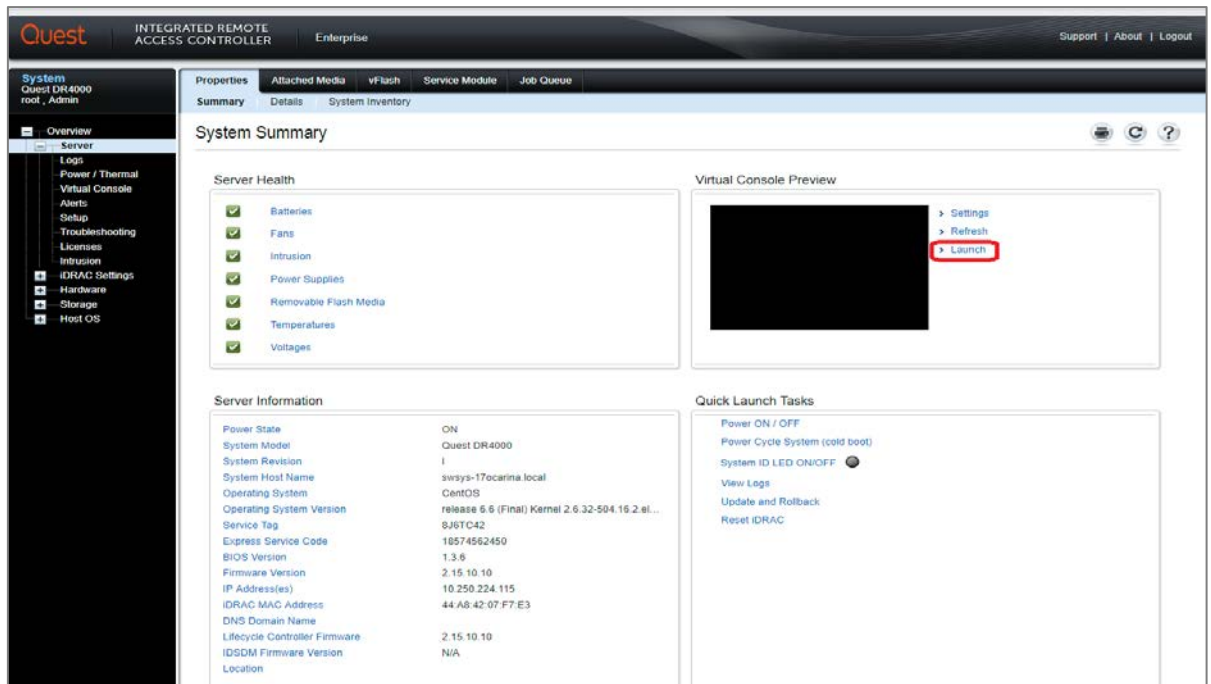
# Installing and configuring the DR Series system

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”**.

The screenshot shows the iDRAC login page for a Quest DR4000 Enterprise system. The page has a dark background with white text. At the top, it says "INTEGRATED REMOTE ACCESS CONTROLLER" and "Enterprise". Below this is a "Login" section with a help icon. The text "iDRAC | Quest DR4000" and "Type the Username and Password and click Submit." is displayed. There are three input fields: "Username:" with "root" entered, "Password:" (empty), and "Domain:" with a dropdown menu showing "This iDRAC". At the bottom right are "Cancel" and "Submit" buttons. The "Username" and "Password" fields are highlighted with red rectangles.

- 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).

```
login as: administrator
administrator@10.250.241.45's password: St0r@ge!
```

- 6 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:

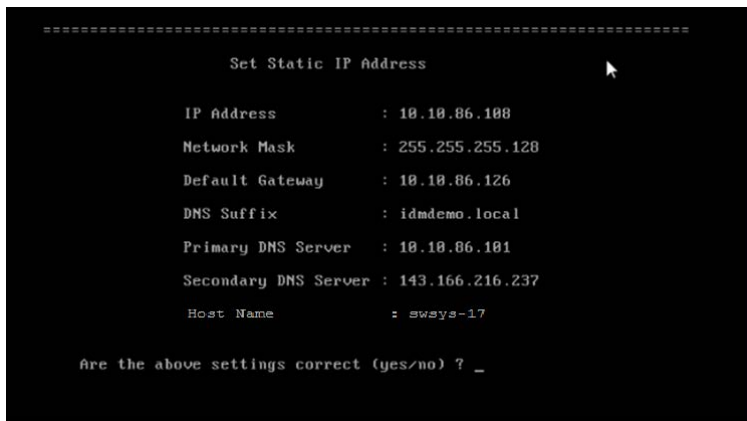
Please enter a DNS Suffix (example: abc.com):

Please enter primary DNS server IP address:

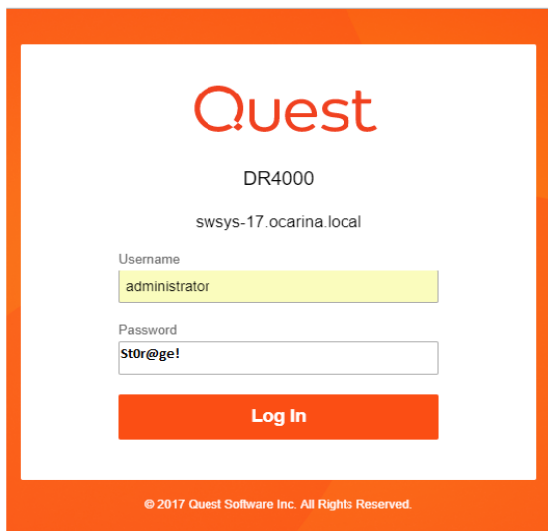
Would you like to define a secondary DNS server (yes/no) ?

Please enter secondary DNS server IP address:
```

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



- 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).

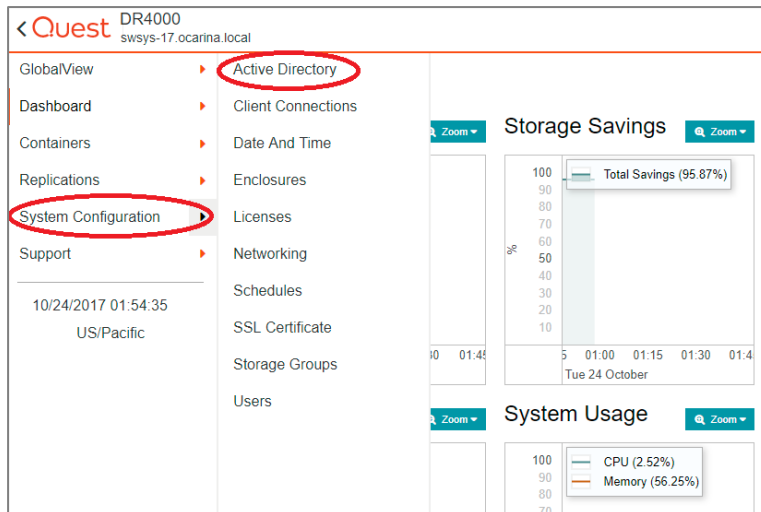


- 9 Join the DR Series system to Active Directory.



**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.

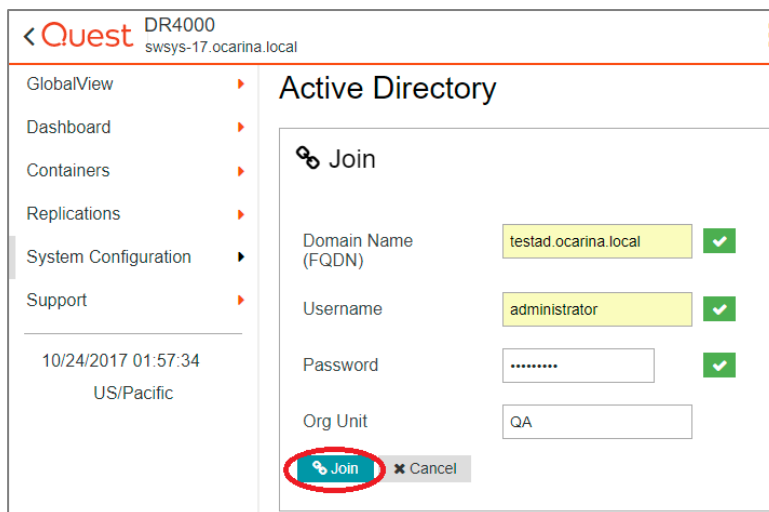
- a Select **Active Directory** in the left navigation area of the GUI.



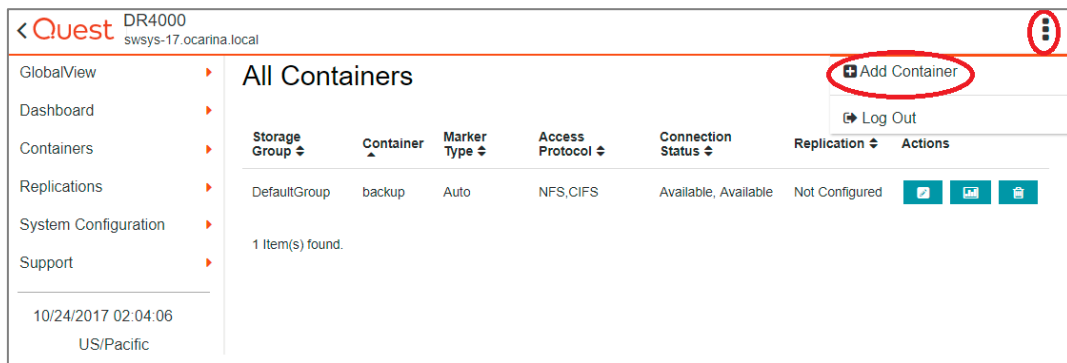
- b Click **join** to enter your Active Directory credentials.



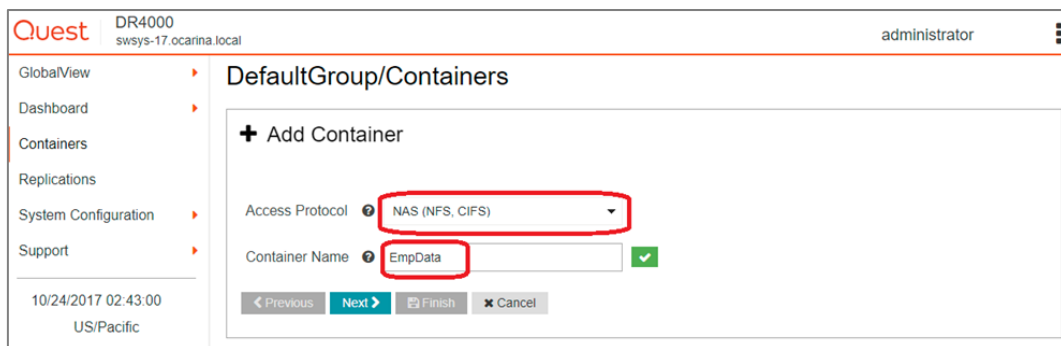
- c Enter your Active Directory credentials.



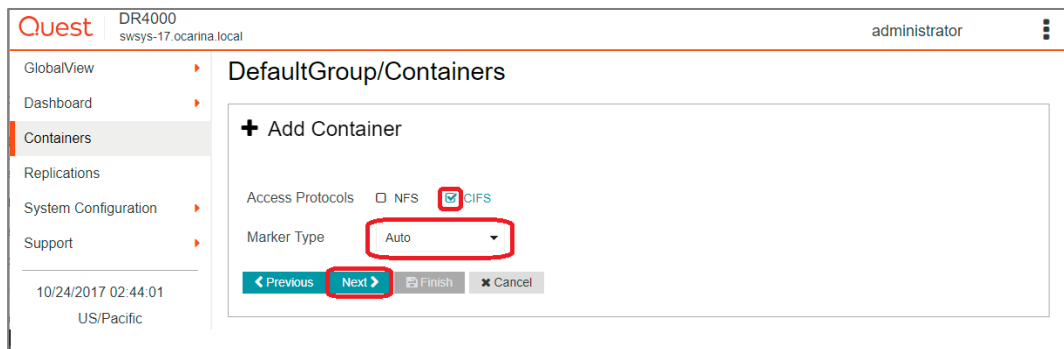
- 10 Create and mount the container as follows. Select **Containers** in the left navigation area of the DR Series system GUI, and then select the **Action Menu** in the upper right corner. Click the **Add Container** option at the top of the menu.



- 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.

Quest DR4000  
swsys-17.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

10/24/2017 02:45:32  
US/Pacific

### DefaultGroup/Containers

#### + Add Container

CIFS Client Access ☒ Open (allow all clients) ☐ Create Client Access List

Client FQDN or IP Address

Allow Clients

< Previous **Next >** Finish Cancel



**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.

Quest DR4000  
swsys-17.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

10/24/2017 02:46:29  
US/Pacific

### DefaultGroup/Containers

#### + Add Container

**Storage Access Protocol**

Access Protocol **NAS (NFS, CIFS)**

Container Name **EmpData**

**Configure NAS Access & Marker**

NAS Access Protocol **CIFS**

Marker Type **Auto**

**Configure CIFS Client Access**

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

< Previous Next **Save** Cancel

13 Confirm that the container has been added.

Quest DR4000  
swsys-17.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

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

### DefaultGroup/Containers

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

2 Item(s) found.

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



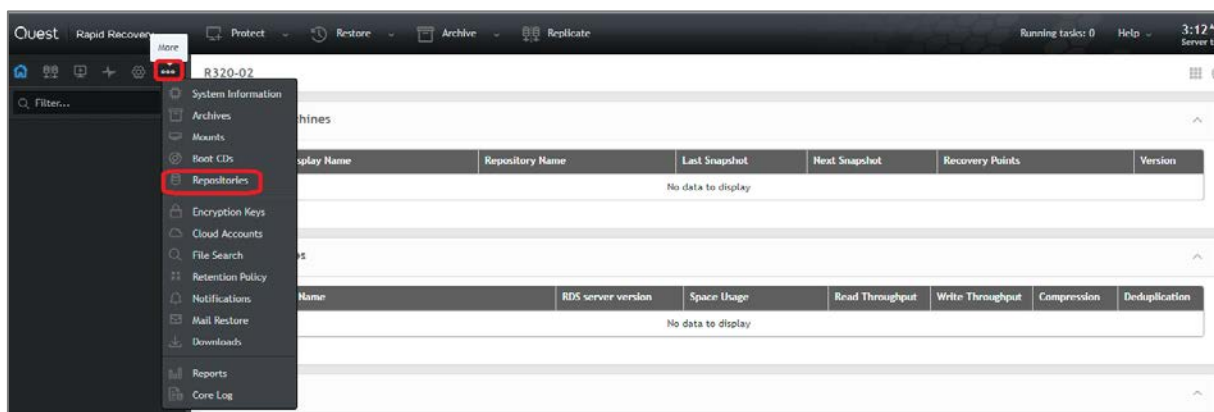
# Setting up AppAssure

## Archiving backup images to the DR Series system

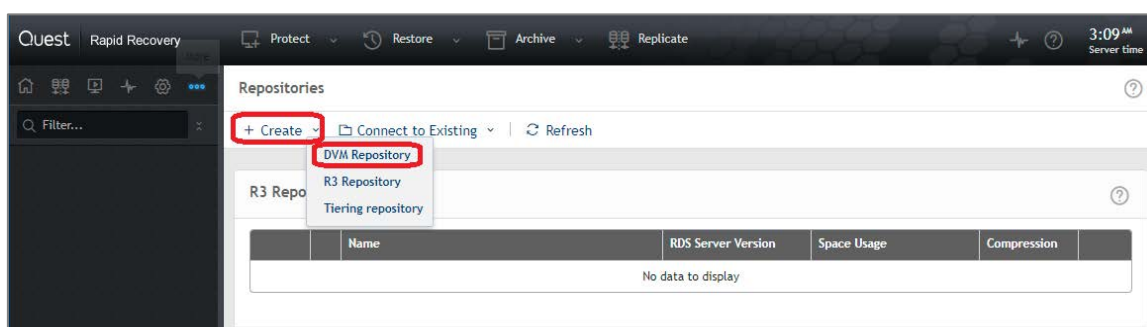
To create a backup job and back up a Windows data set, follow steps 1-10 in the procedure that follows. If you already have a backed up data set, skip steps 1-10 and start from step 11 to archive the backup data set to the DR Series system.

**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**.

Quest | Rapid Recovery | Protect | Restore | Archive | Replicate

Filter...

### Add New Repository

Details

Repository name:  Comments:

Concurrent operations:

Storage Locations

+ Add Storage Location

Data Path	Metadata Path	Size
No data to display		

Create Cancel

- 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).

Quest | Rapid Recovery | Protect | Restore | Archive | Replicate

Filter...

### Add New Repository

Details

Repository name:  Comments:

Concurrent operations:

Storage Locations

+ Add Storage Location

Data Path	Metadata Path	Size
No data to display		

Create Cancel

### Add Storage Location

Storage Location

☐ Add file on local disk ☒ Add file on CIFS share

UNC path:

User name:

Password:

Storage Configuration [More Details](#)

Size:

'More Details' allows editing of additional 'Storage Location' parameters. Before changing the defaults, please refer to the documentation.

Save Cancel

- 5 Click **Create**.

Quest | Rapid Recovery | Protect | Restore | Archive | Replicate

Filter...

### Add New Repository

Details

Repository name:  Comments:

Concurrent operations:

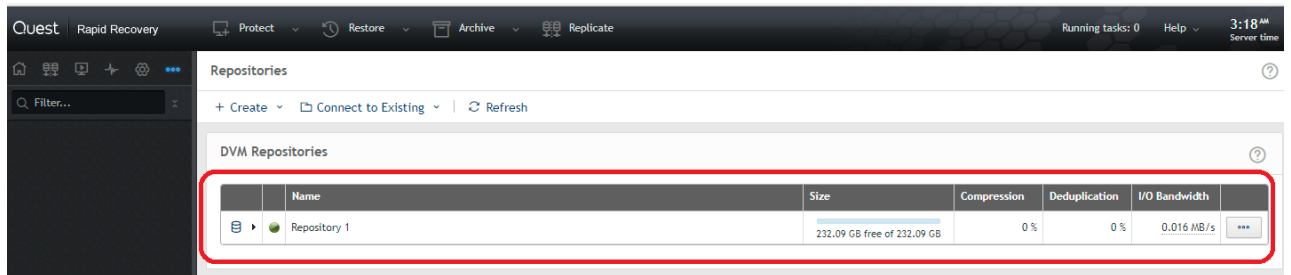
Storage Locations

+ Add Storage Location

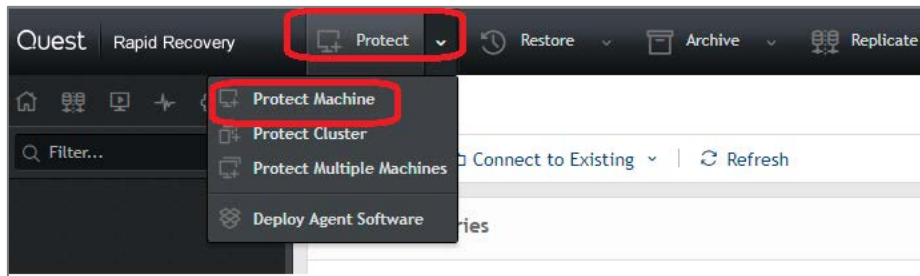
Data Path	Metadata Path	Size
\\10.250.241.45\EmpData	\\10.250.241.45\EmpData	250 GB

Create Cancel

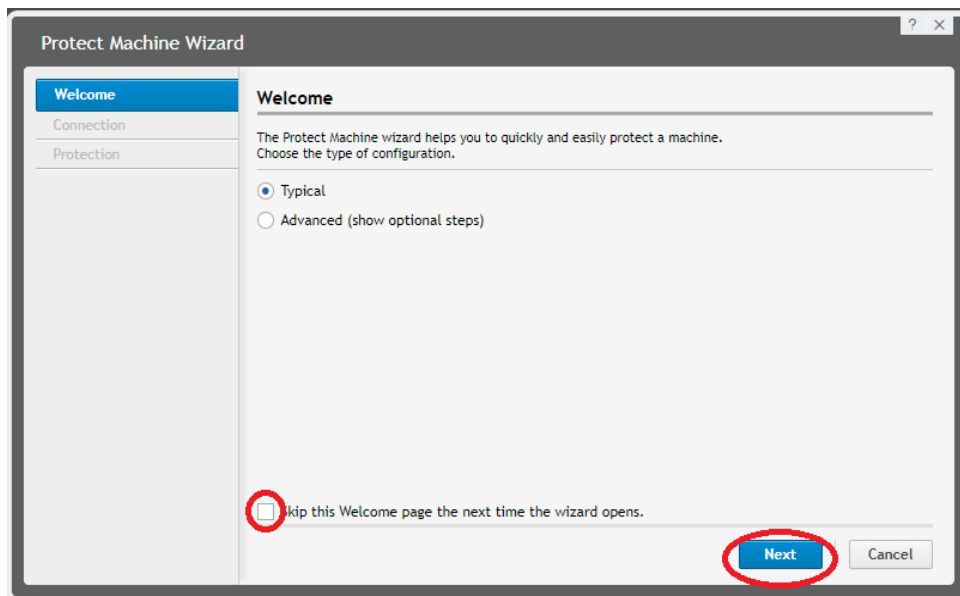
- 6 Verify the Repository has been created in the list of DVM repositories.



- 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**.

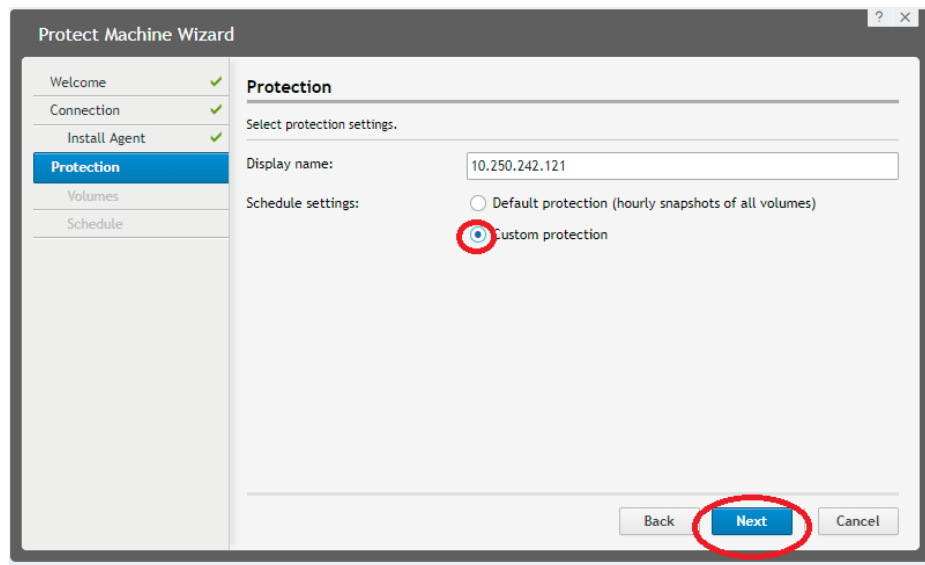
The screenshot shows the 'Protect Machine Wizard' window at the 'Connection' step. The left sidebar has 'Welcome' (checked), 'Connection' (selected), and 'Protection'. The main area is titled 'Connection' and contains the instruction 'Click Next to connect to the machine you want to protect.' Below this are fields for 'Operating system' (Windows), 'Host' (10.250.242.121), 'Port' (8006), 'User name' (testad\administrator), and 'Password' (masked with dots). At the bottom right, the 'Next' button is circled in red.

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

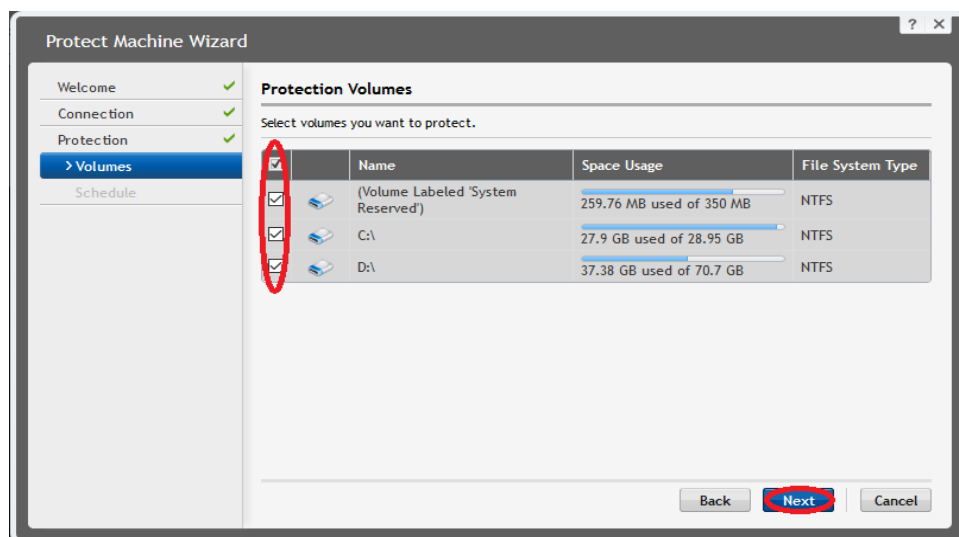
The screenshot shows the 'Protect Machine Wizard' window at the 'Protection' step. The left sidebar has 'Welcome' (checked), 'Connection' (checked), 'Install Agent' (checked), and 'Protection' (selected). The main area is titled 'Protection' and contains the instruction 'Select protection settings.' Below this are fields for 'Display name' (10.250.242.121) and 'Schedule settings'. Under 'Schedule settings', the 'Default protection (hourly snapshots of all volumes)' radio button is selected and circled in red. The 'Custom protection' radio button is unselected. At the bottom right, the 'Finish' button is circled in red.

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**.

**Protect Machine Wizard**

Welcome ✓  
Connection ✓  
Protection ✓  
Volumes ✓  
Schedule

**Protection Schedule**

Set protection schedule. In order to use advanced schedule options, click "Initially pause protection" and modify settings later from the Agent Summary page.

**Periods**

☒ Weekdays (Mon-Fri)  
From: 12:00 AM To: 11:59 PM Every: 60 minutes  
☐ Take snapshots the rest time Every: 60 minutes

☒ Weekends (Sat, Sun) Every: 60 minutes

☐ Daily protection time: 12:00 PM

☐ Initially pause protection

Back **Finish** Cancel

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

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

**Protect Machine Wizard**

Welcome ✓  
Connection  
Protection  
Repository  
Encryption

**Connection**

Click Next to connect to the machine you want to protect.

Host: 10.250.242.127  
Port: 8006  
User name: testadadministrator  
Password: .....

Back **Next** Cancel

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

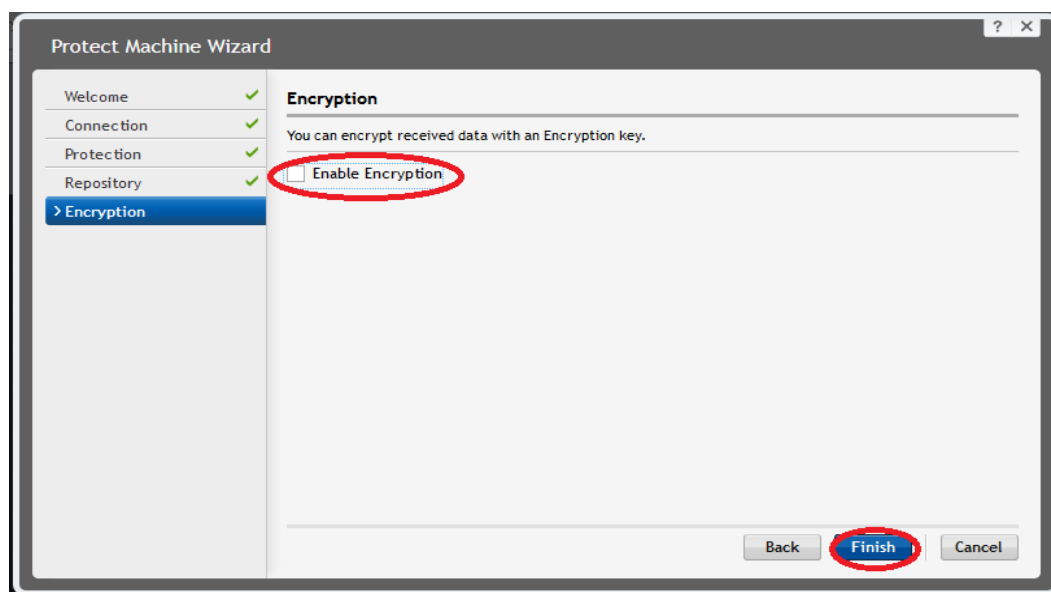
The screenshot shows the 'Protect Machine Wizard' window at the 'Protection' step. The left sidebar has 'Protection' selected. The main area is titled 'Protection' and 'Select protection settings.' It includes a 'Display name' field with '10.250.242.127'. Under 'Schedule Settings', the 'Default protection (hourly snapshots of all volumes)' radio button is selected and circled in red. The 'Custom protection' radio button is unselected. At the bottom right, the 'Next' button is highlighted with a red circle.

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

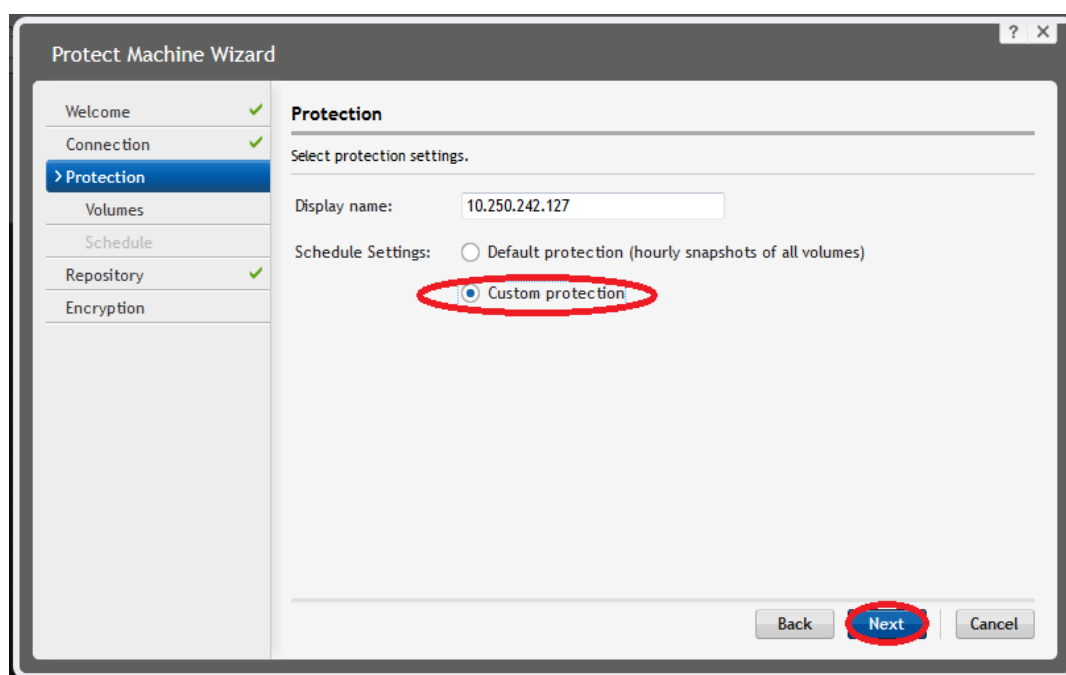
- ☐ **Use an existing repository** - To select an existing repository.
- ☐ **Create new repository** – To create a new repository.

The screenshot shows the 'Protect Machine Wizard' window at the 'Repository' step. The left sidebar has 'Repository' selected. The main area is titled 'Repository' and 'Specify the location for storing the protected data.' It has two radio buttons: 'Use an existing Repository' (selected and circled in red) and 'Create a Repository' (unselected and circled in red). Below 'Use an existing Repository' is a dropdown menu showing 'Repository 1'. Below 'Create a Repository' are fields for 'Name', 'Location', 'User name' (with a hint 'Required for network path only'), 'Password', and 'Metadata Path'. At the bottom right, the 'Next' button is highlighted with a red circle.

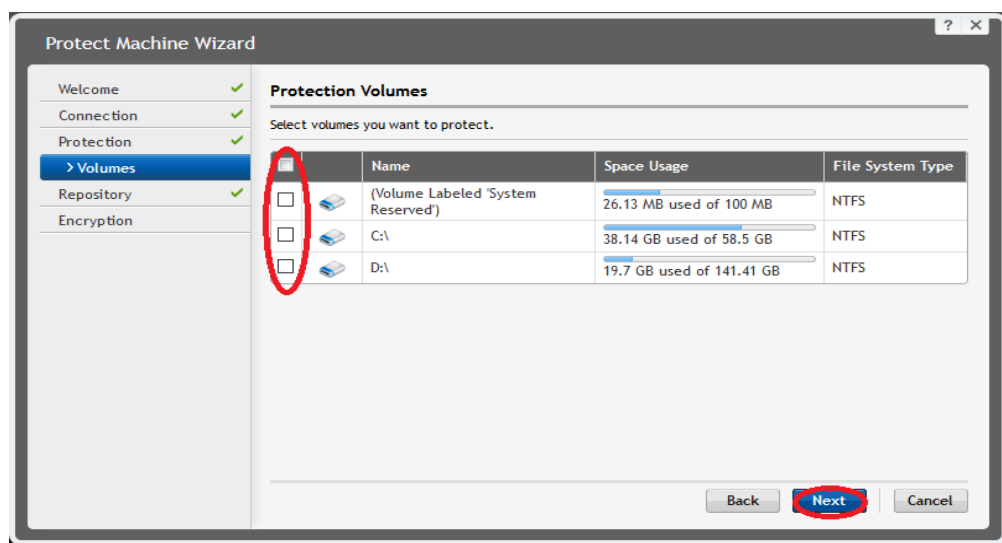
- d To encrypt data during protection, select **Enable Encryption** and click **Finish**; otherwise, click **Finish**.



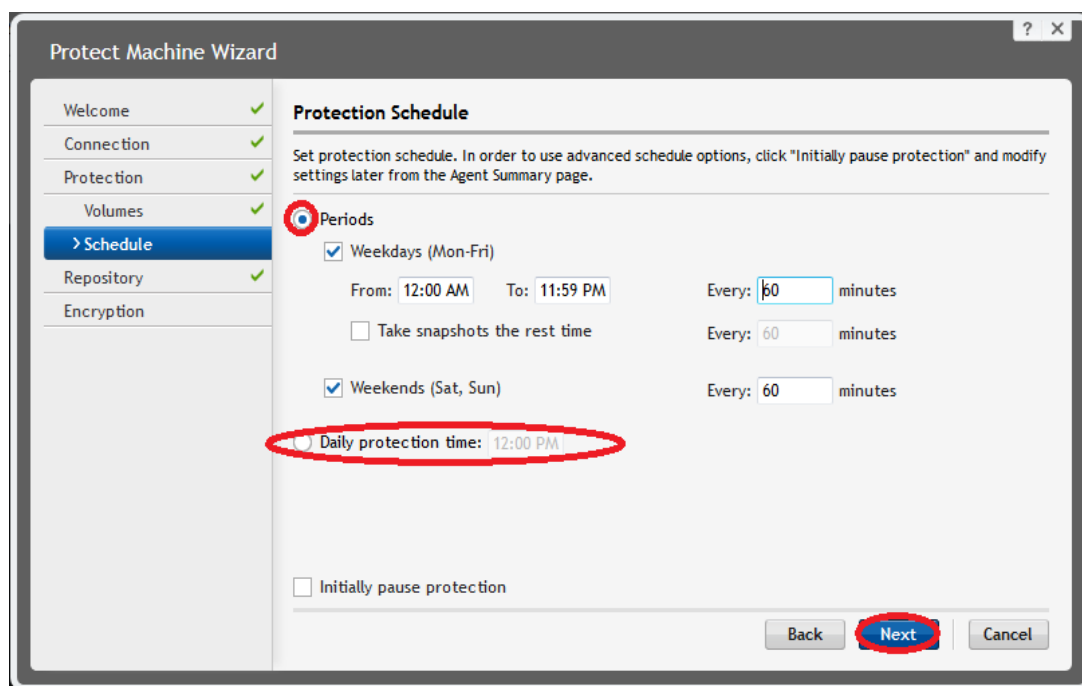
- e Select the **Custom Protection** option and click **Next**.



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

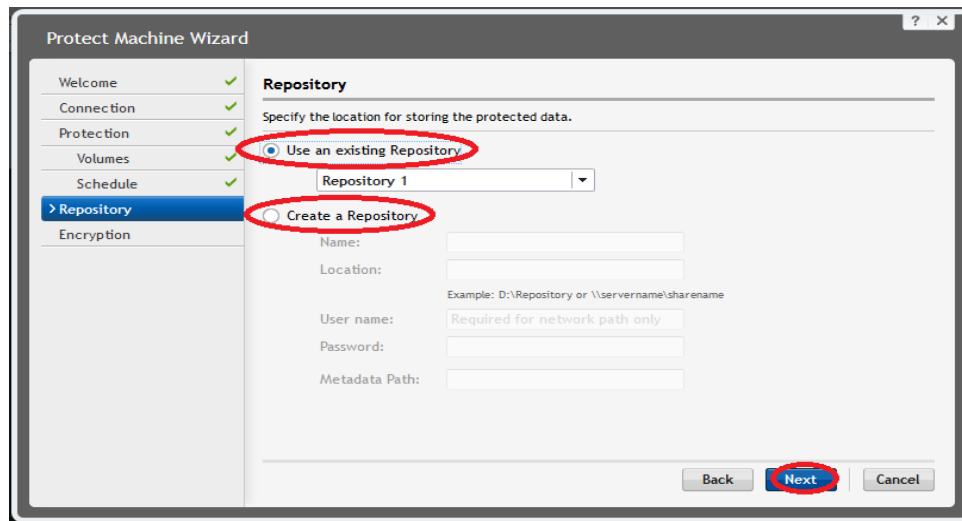


- g Select the appropriate protection schedule and click **Next**.

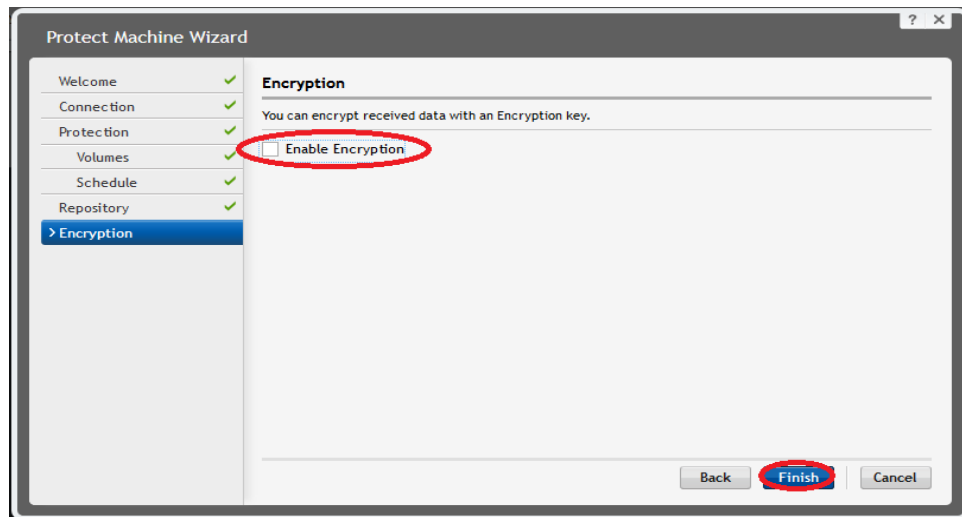


h Select one of the following options for the location for storing protected data and click **Save**:

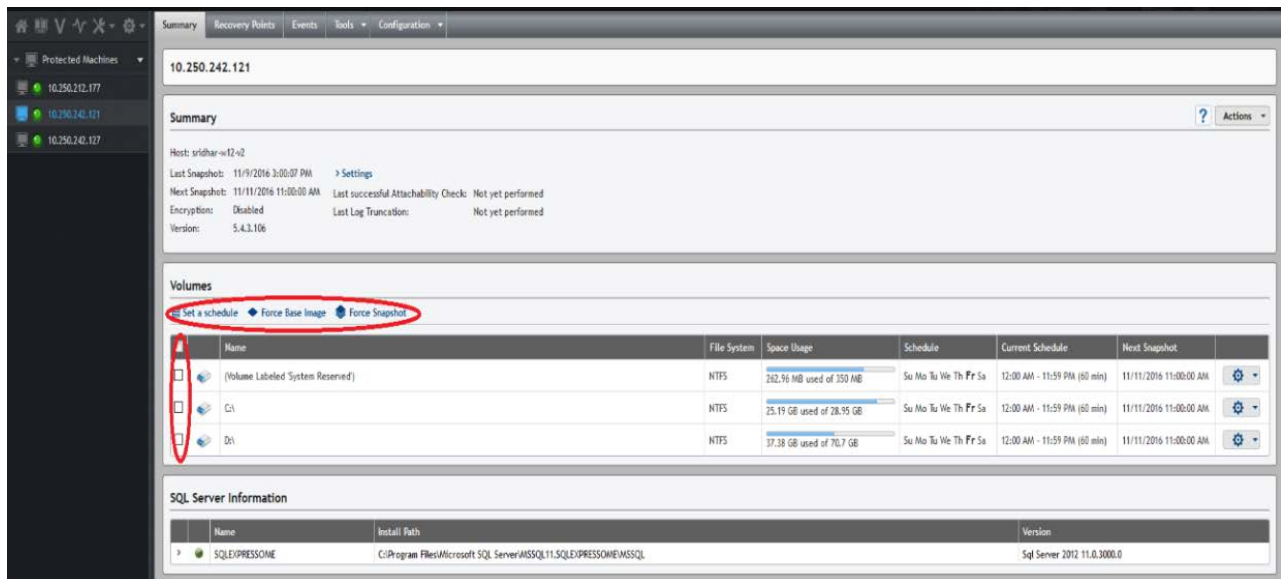
- ☐ **Use an existing repository** - To select an existing repository.
- ☐ **Create new repository** – To create a new repository.



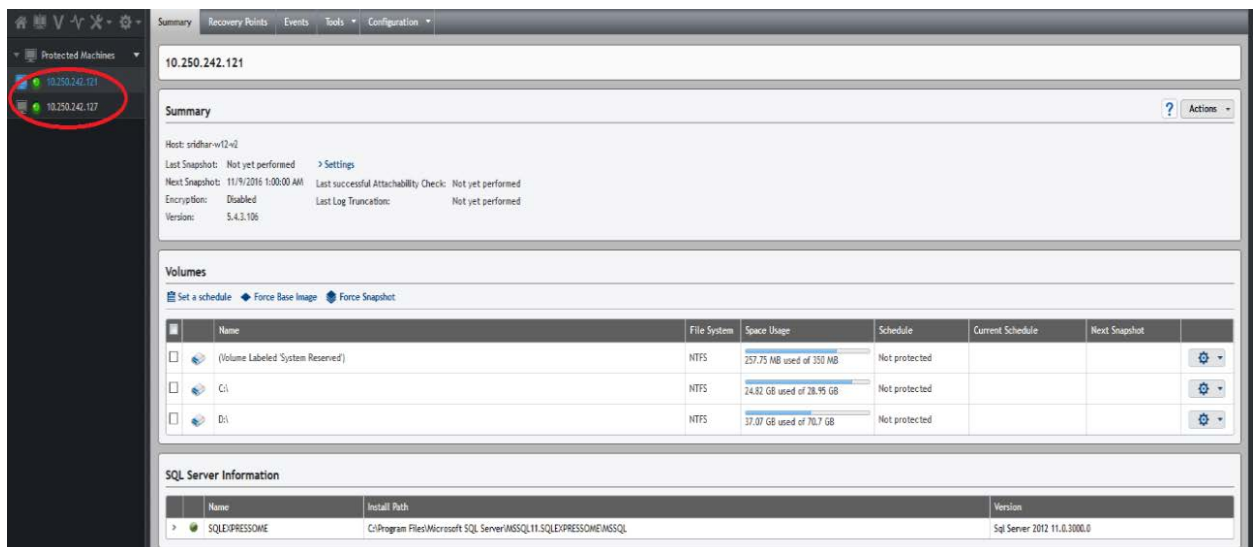
i If you want to encrypt the data during the protection, select **Enable Encryption** and click **Finish**; otherwise, click **Finish**.



- 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**.

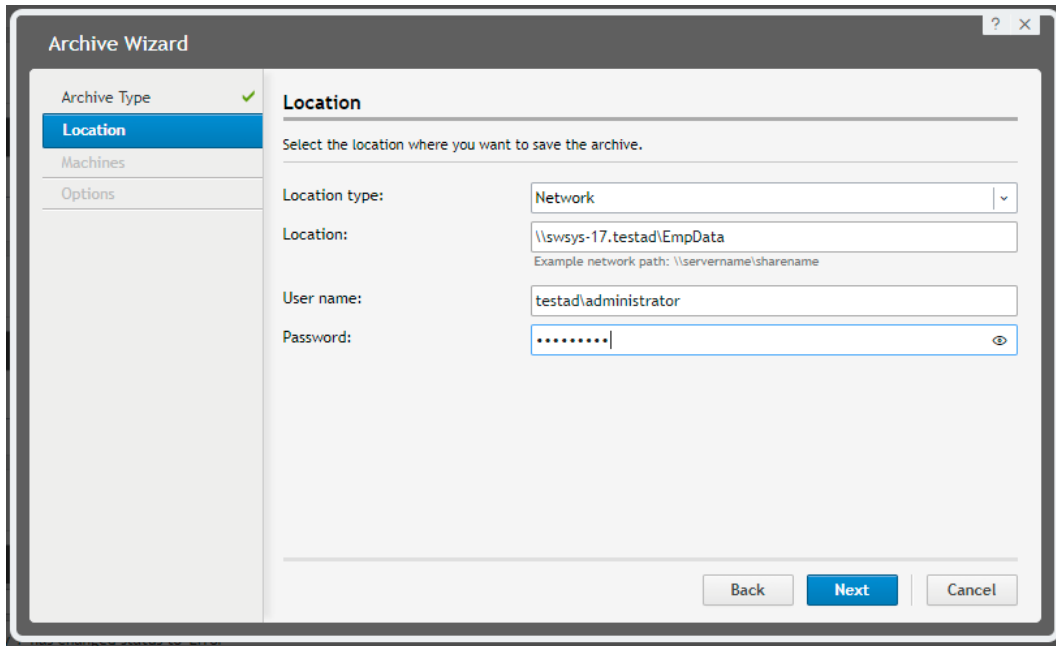
The screenshot shows the AppAssure 6.2 interface. In the left sidebar, under 'Protected Machines', the machine with IP address 10.250.242.127 is selected and circled in red. The main window displays the 'Recovery Points' tab for this machine. The summary section shows: Total Recovery Points: 63, Total Protected Data: 144.7 GB, Repository: Repository 1, Passed Checks Count: 0, Required Checks Count: 0, Failed Checks Count: 0, and Repository Status: 137.05 GB used of 9.28 TB. Below the summary is a table of recovery points.

Status	Encrypted	Contents	Type	Creation Date	Size
>		(Volume Labeled System Reserved), D:\	Incremental	11/11/2016 3:00:00 AM	513.55 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/11/2016 12:13:02 AM	928.09 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 11:00:01 PM	5.11 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 10:00:01 PM	5.03 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 9:00:03 PM	5.05 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 8:00:01 PM	5.08 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 7:00:01 PM	5.02 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 6:00:02 PM	5.02 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 5:00:02 PM	5.05 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 4:00:05 PM	5.12 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 3:00:02 PM	5.21 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 2:00:06 PM	5.26 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 1:00:03 PM	5.19 MB
>		(Volume Labeled System Reserved), D:\	Incremental	11/9/2016 12:00:05 PM	5.11 MB

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

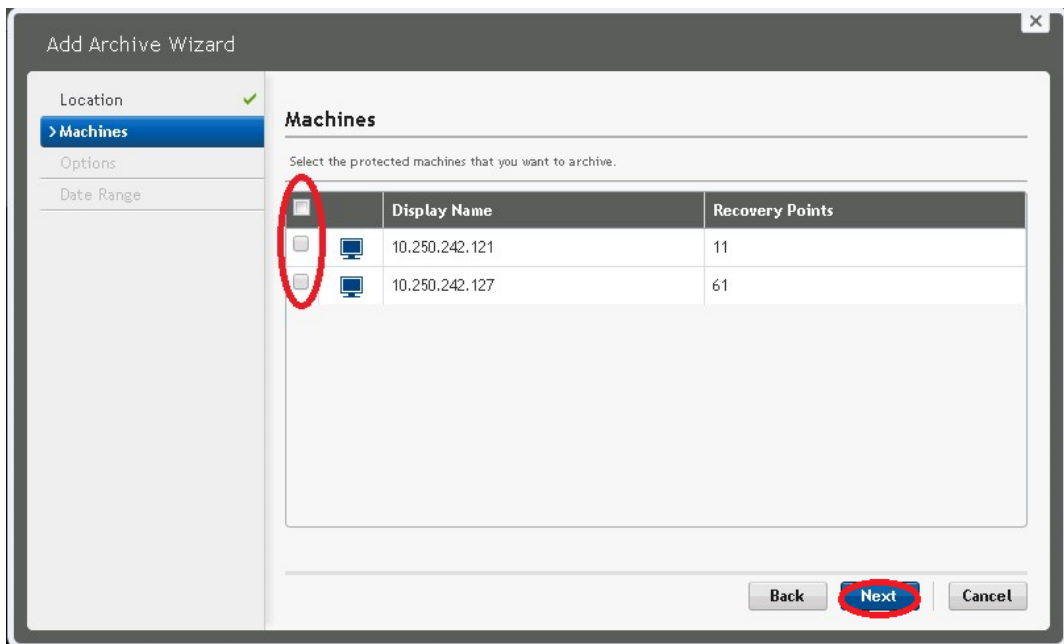
The screenshot shows the AppAssure 6.2 interface. The top navigation bar includes 'Quest', 'Rapid Recovery', 'Protect', 'Restore', 'Archive', and 'Replicate'. The 'Archive' dropdown menu is open, showing three options: '+ Create Archive' (highlighted with a red box), 'Import Archive', and 'Attach Archive'. Below the menu, the 'Protected Machines' section is visible, showing a table with columns: Display Name, Repository Name, Last Snapshot, and Next Snapshot. The table is currently empty, displaying 'No data to display'.

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



The Archive Wizard window shows the 'Location' step. The left sidebar has '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' (dropdown menu set to 'Network'), 'Location' (text box containing '\\swsys-17.testad\EmpData' with a hint 'Example network path: \\servername\sharename'), 'User name' (text box containing 'testad\administrator'), and 'Password' (password box with seven dots and an eye icon). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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



The 'Add Archive Wizard' window shows the 'Machines' step. The left sidebar has '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 column, 'Display Name', and 'Recovery Points'. The table lists two machines. The first checkbox is circled in red. At the bottom right are 'Back', 'Next' (circled in red), and 'Cancel' buttons.

	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**.

The screenshot shows the 'Add Archive Wizard' dialog box with the 'Options' step selected in the left sidebar. The 'Options' section has a title bar and a subtitle 'Select recycle options for archive.' Below this, there are three main settings: 'Maximum Size' set to 'Entire Target', 'Recycle action' set to 'Do not reuse' (highlighted with a red circle), and 'Comment' set to an empty text box. At the bottom, there is a 'Use compatible format' checkbox and a note: 'NOTE: The New format offers better performance however it is not compatible with older Cores.' The 'Next' button is highlighted with a red circle.

Location ✓  
Machines ✓  
Options  
Date Range

**Options**

Select recycle options for archive.

Maximum Size: ☒ Entire Target ☐ 0 MB

Recycle action: **Do not reuse**  
Do not reuse  
Replace this Core  
Erase completely  
Incremental

Comment:

Use compatible format: ☐ NOTE: The New format offers better performance however it is not compatible with older Cores.

Back Next Cancel

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

The screenshot shows the 'Add Archive Wizard' dialog box with the 'Date Range' step selected in the left sidebar. The 'Date Range' section has a title bar and a subtitle 'Select date range for recovery points which will be included in archive.' Below this, there are two date pickers: 'Start Date' set to '12:00 AM 01/01/2016' and 'Expired On' set to '12:00 AM 06/30/2016' (both highlighted with a red circle). The 'Finish' button is highlighted with a red circle.

Location ✓  
Machines ✓  
Options ✓  
Date Range

**Date Range**

Select date range for recovery points which will be included in archive.

Start Date: 12:00 AM 01/01/2016

Expired On: 12:00 AM 06/30/2016

Back Finish Cancel

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

The screenshot shows the AppAssure 6.2 interface. The 'Events' tab is selected in the top navigation bar. Below the navigation bar, there is a 'Tasks' section with tabs for 'Tasks', 'Alerts', and 'Events'. The 'Events' tab is active, displaying a list of tasks. The task 'Archive of 1 Agents (10.250.242.127) from 11/1/2016 12:00:00 AM to 11/10/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata' is highlighted. A 'Monitor Active Task' dialog is open, showing the progress of this task. The dialog includes a progress bar at 1%, a 'Details' section with elapsed time, rate, and time remaining, and a 'Cancel' button.

Job	Status	Start Time	End Time	Details
Maintaining repository Repository 2	0% of 100%	11/11/2016 1:00:03 AM		
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.121'		11/11/2016 1:00:02 AM		
Checking backup on \\DR6300-22.testad.ocarina.local\empdata	Succeeded	11/11/2016 12:04:39 AM	11/11/2016 12:04:39 AM	
Archive of 2 Agents (10.250.242.121, 10.250.242.127) from 11/1/2016 12:00:00 AM to 11/11/2016 12:00:00 AM. Archive path: \\DR6300-22.testad.ocarina.local\empdata	Succeeded	11/11/2016 12:13:02 AM	11/11/2016 12:13:05 AM	
Archive of 1 Agents (10.250.242.127) from 11/1/2016 12:00:00 AM to 11/10/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata	1.24 GB of 143.3 GB	11/11/2016 12:13:02 AM		

**Monitor Active Task**

Archive of 1 Agents (10.250.242.127) from 11/1/2016 12:00:00 AM to 11/10/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata

Start Time: 11/11/2016 12:13:02 AM

Progress: 1%

**Details**

Elapsed Time: 2 hours, 12 minutes, 32 seconds  
Rate: 256.66 KB/s  
Time Remaining: -

Progress: 1.24 GB of 143.3 GB  
Phase: Running archive

> Cancel

Open in New Window

Close (Task will run in background)

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

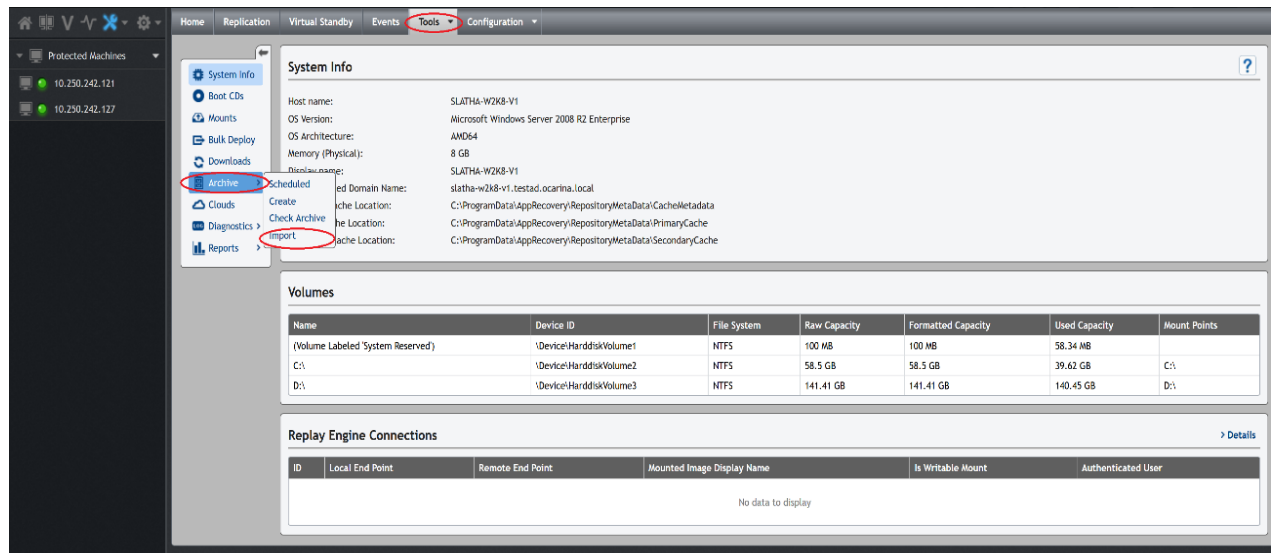
The screenshot shows the AppAssure 6.2 interface with the 'Events' tab selected. The 'Tasks' section displays a list of tasks. The task 'Archive of 1 Agents (10.250.242.127) from 11/1/2016 12:00:00 AM to 11/10/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata' is highlighted with a red circle. The task status is '1.31 GB of 143.3 GB'.

Job	Status	Start Time	End Time	Details
Maintaining repository Repository 2	0% of 100%	11/11/2016 1:00:03 AM		
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.121'		11/11/2016 1:00:02 AM		
Checking backup on \\DR6300-22.testad.ocarina.local\empdata	Succeeded	11/11/2016 12:04:39 AM	11/11/2016 12:04:39 AM	
Archive of 2 Agents (10.250.242.121, 10.250.242.127) from 11/1/2016 12:00:00 AM to 11/11/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata	Succeeded	11/11/2016 12:13:02 AM	11/11/2016 12:13:05 AM	
Archive of 1 Agents (10.250.242.127) from 11/1/2016 12:00:00 AM to 11/10/2016 12:00:00 AM. Archive path: \\swws-17.testad.ocarina.local\empdata	1.31 GB of 143.3 GB	11/11/2016 12:13:02 AM		
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	403.96 MB of 40.96 GB	11/11/2016 12:13:02 AM		
Rolling up 2 protected machine(s).	Canceled	...	...	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 11:00:01 PM	11/9/2016 11:27:05 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 10:00:01 PM	11/9/2016 10:27:07 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 9:00:03 PM	11/9/2016 9:27:09 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Error	11/9/2016 8:00:01 PM	11/9/2016 8:27:01 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 7:00:01 PM	11/9/2016 7:27:05 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 6:00:02 PM	11/9/2016 6:26:57 PM	
Transfer of volumes [Volume Labeled System Reserved], C:\, D:\ from '10.250.242.127'	Succeeded	11/9/2016 5:00:02 PM	11/9/2016 5:27:00 PM	

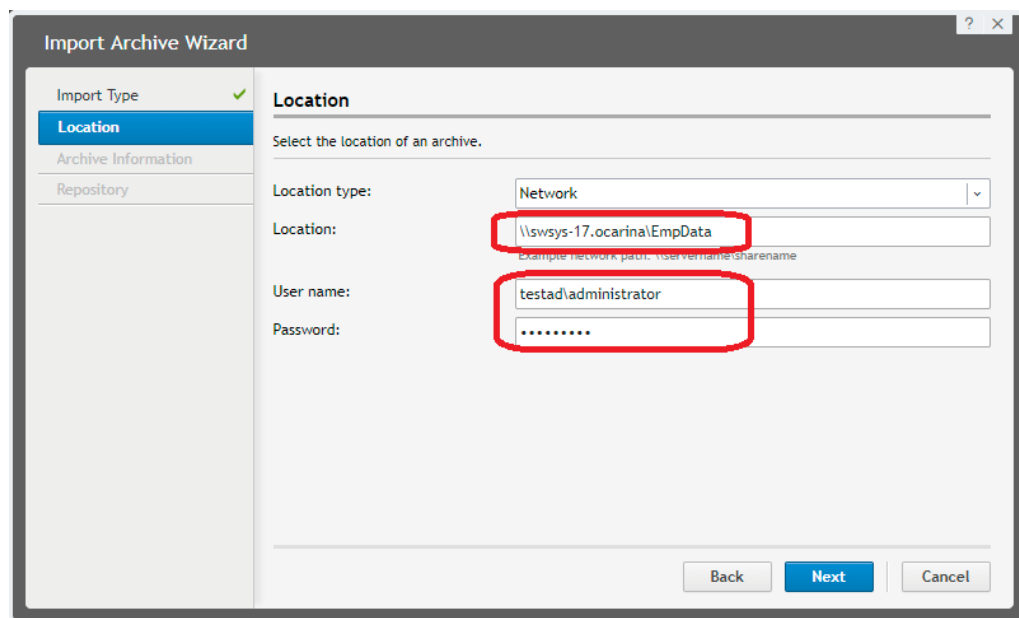
# Restoring archived backup images from the DR Series system

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

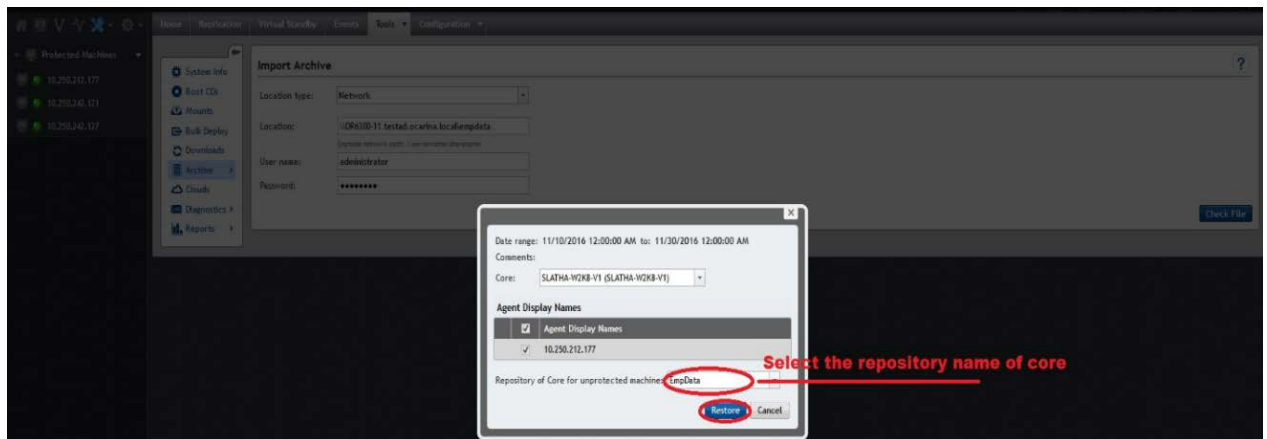
- 1 Click **Tools > Archive > Import**.



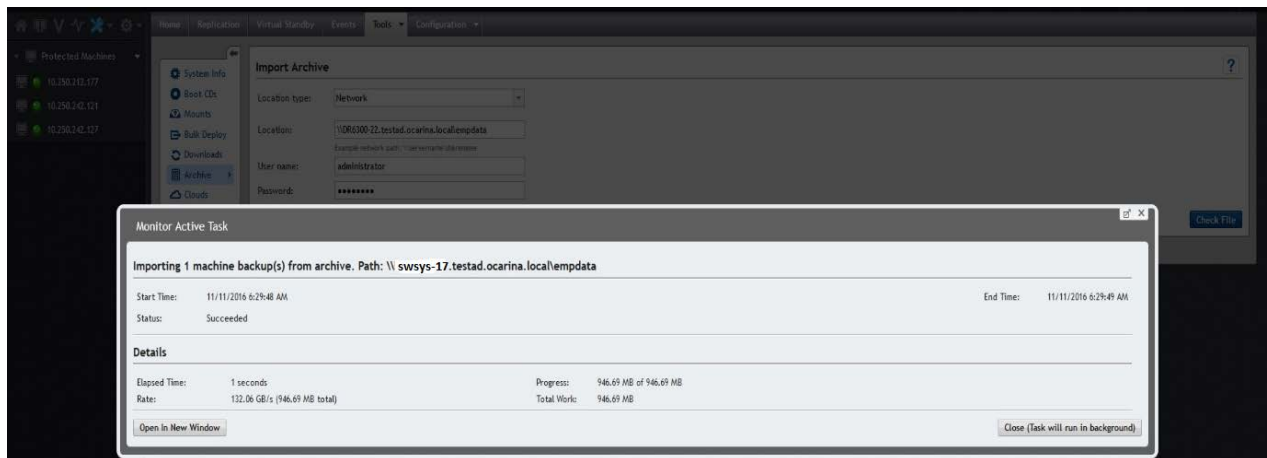
- 2 Enter the UNC path of the DR container share that holds the archive images. In addition, enter the CIFS credentials for authenticating to the DR Series system. Click **Check File**.



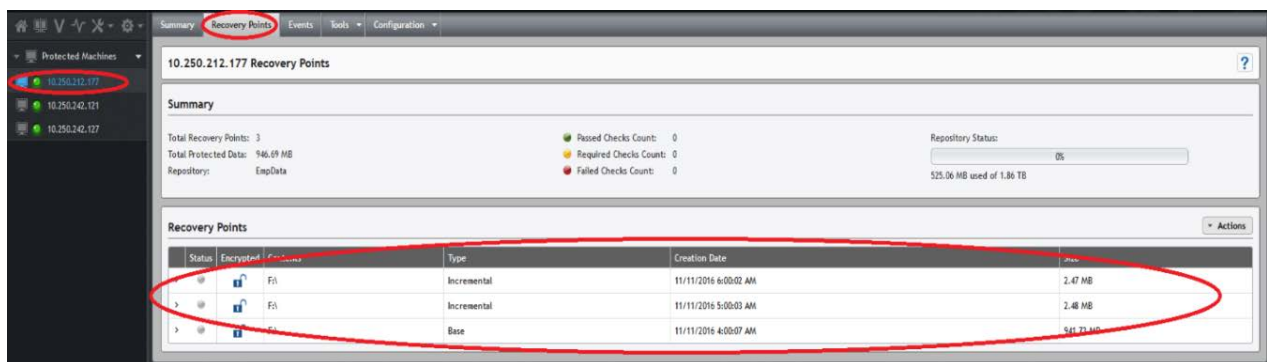
- 3 Under **Agent Names**, select the agent and repository that the archived data will be imported to and click **Restore**.



- 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.

The screenshot displays the AppAssure 6.2 web interface. On the left, a sidebar lists 'Protected Machines' with three entries: 10.250.212.177, 10.250.240.131, and 10.250.240.127. The main content area is titled '10.250.212.177 Recovery Points'. It features a 'Summary' section with metrics: Total Recovery Points: 3, Total Protected Data: 946.69 MB, Repository: EmpData, Passed Checks Count: 0, Required Checks Count: 0, Failed Checks Count: 0, and Repository Status: 0% (525.06 MB used of 1.86 TB). Below this is the 'Recovery Points' table with columns: Status, Encrypted, Contents, Type, Creation Date, and Size. A single row is shown with a minus icon in the Status column, which is circled in red. To the right of the table, the 'Actions' section contains 'Mount', 'Export', and 'Restore' buttons, also circled in red. Below the actions is a 'Contents' section with a table showing the file structure: F:\, Incremental, 2.47 MB.

Status	Encrypted	Contents	Type	Creation Date	Size
-		F:\	Incremental	11/11/2016 6:00:02 AM	2.47 MB

Status	Title	Type	Size
>	F:\	Incremental	2.47 MB

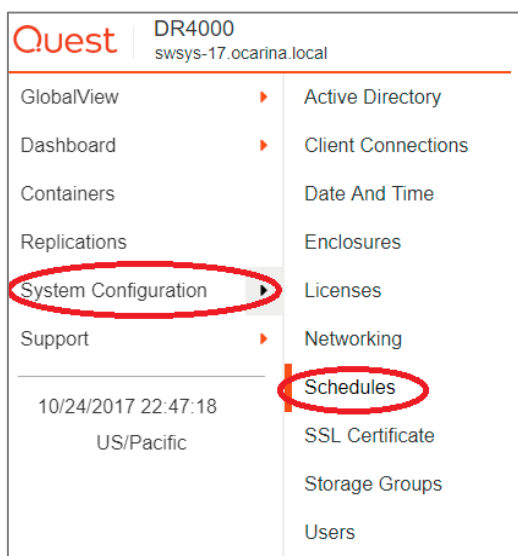
Status	Contents	Type	Creation Date	Size
>	F:\	Incremental	11/11/2016 5:00:03 AM	2.48 MB
>	F:\	Base	11/11/2016 4:00:07 AM	941.73 MB

## 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**.

Quest DR4000 swsys-17.ocarina.local administrator

GlobalView Dashboard Containers Replications System Configuration Support

10/24/2017 22:43:43 US/Pacific

## Schedules

Cleaner status: **Done** ■ Cleaner Schedule All ■ Source Replication Schedule All ■ Target Replication Schedule All

	Sun	Mon	Tue	Wed	Thu	Fr
3:00						
4:00						
5:00						

- + Add Cleaner Event
- + Add Replication Event
- + Add Multiple Replications
- + Add Multiple Cleaners
- + Run Cleaner Now
- Log Out

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

Quest DR4000 swsys-17.ocarina.local administrator

GlobalView Dashboard Containers Replications System Configuration Support

10/24/2017 22:44:24 US/Pacific

## Schedules

Cleaner status: **Done** ■ Cleaner Schedule All ■ Source Replication Schedule All ■ Target Replication Schedule All

**New**

Only one cleaner event is allowed per day.

Set event from start day ▼ at: -- : -- to end day ▼ at: -- : --

Save Cancel

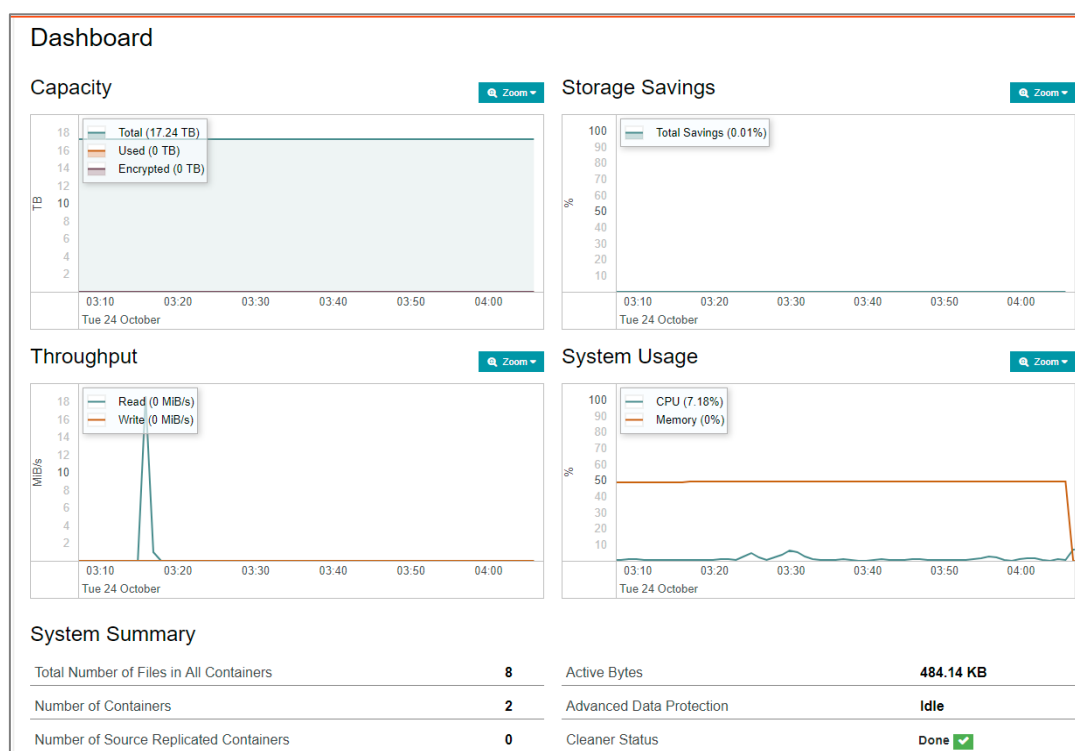
For additional guidance on setting up the system cleaner, refer to the white paper, *DR Series Cleaner Best Practices*. You can download this document from the [DR Series support site](#) by selecting your specific DR Series system model, and then navigating to the Technical Documentation page.

# 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.

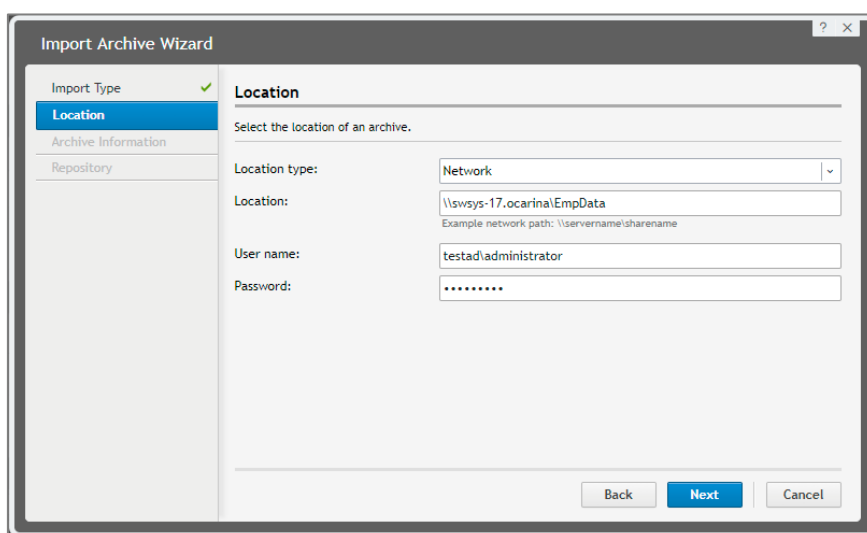


**NOTE:** Deduplication ratios increase over time. It is not uncommon to see a 2-4x reduction (25-50% total savings) on the initial backup. As additional full backup jobs are completed, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio, in most cases.



## 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.



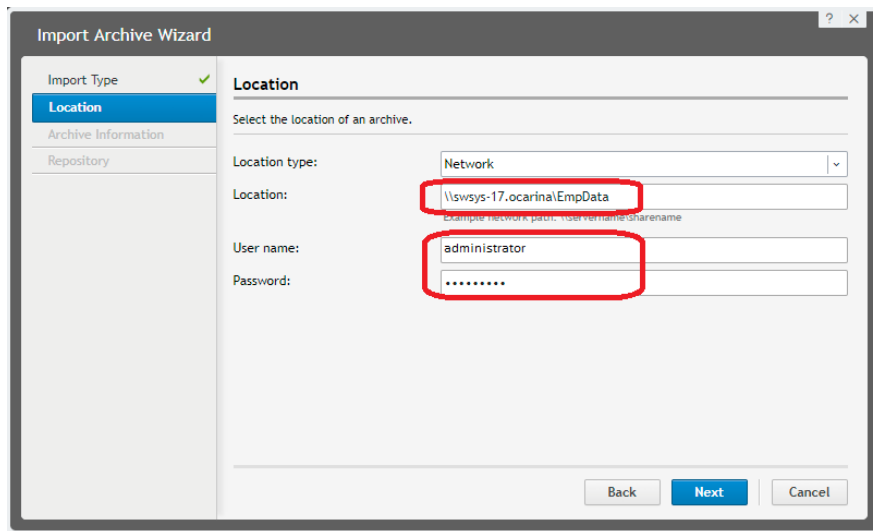
The screenshot shows the 'Import Archive Wizard' dialog box with the 'Location' tab selected. The 'Import Type' is marked with a green checkmark. The 'Location' tab is highlighted in blue. The 'Location' section contains the following fields:

- Location type:** A dropdown menu set to 'Network'.
- Location:** A text box containing '\\swsys-17.ocarina\EmpData'. Below it, a small text box shows the example network path: '\\servername\sharename'.
- User name:** A text box containing 'testad\administrator'.
- Password:** A text box with masked characters (dots).

At the bottom of the dialog box are three buttons: 'Back', 'Next', and 'Cancel'.



**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.

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

- 1 Create a new user for Linux Agent:
- 2 Set a password for the new user:
- 3 Add the user to the root, daemon, adm, and wheel groups.

```
useradd approot
```

```
passwd approot
```

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

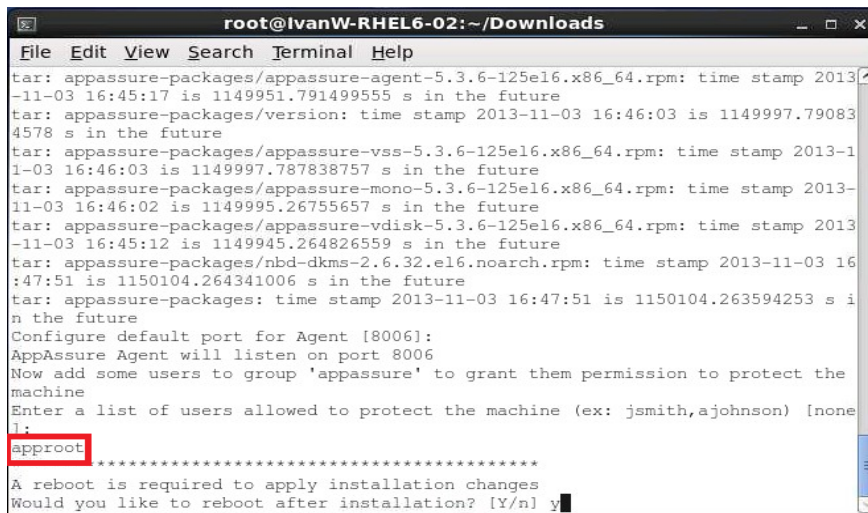
```

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
```



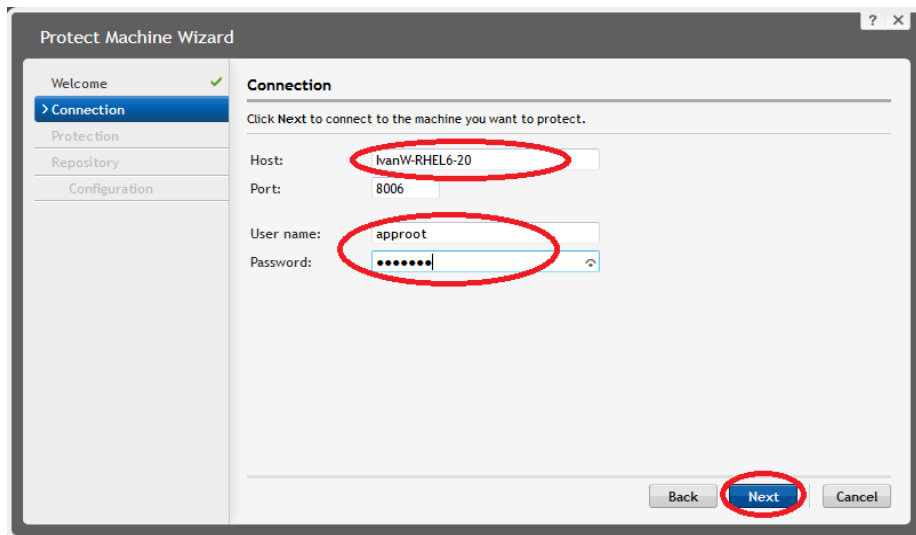
```
root@IvanW-RHEL6-02:~/Downloads
tar: appassure-packages/appassure-agent-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:45:17 is 1149951.791499555 s in the future
tar: appassure-packages/version: time stamp 2013-11-03 16:46:03 is 1149997.790834578 s in the future
tar: appassure-packages/appassure-vss-5.3.6-125el6.x86_64.rpm: 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/nbd-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]
l:
aproot
*****
A reboot is required to apply installation changes
Would you like to reboot after installation? [Y/n] y
```

**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**.



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