



Setting Up the Dell™ DR Series System as an Archive Target on AppAssure 5.3.6

Dell Engineering
January 2014

Revisions

Date	Description
January 2014	Initial release

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.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. 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. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

Revisions.....	2
Executive summary	4
1 Install and Configure the DR Series System.....	5
2 Set up AppAssure	12
2.1 Archive backup images to the DR Series system	12
2.2 Restore archived backup images from the DR Series system.....	18
3 Set up the DR Series system cleaner.....	21
4 Monitoring deduplication, compression, and performance.....	22
A Appendix.....	23
A.1 Configure the DR container share as a CIFS storage device on AppAssure	23
A.2 Back up a Linux client.....	24
A.2.1 Install the Linux agent onto the client machine	24
A.2.2 Back up the Linux client machine	25



Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for AppAssure 5.3.6. This document is a quick reference guide and does not include all DR Series system deployment best practices.

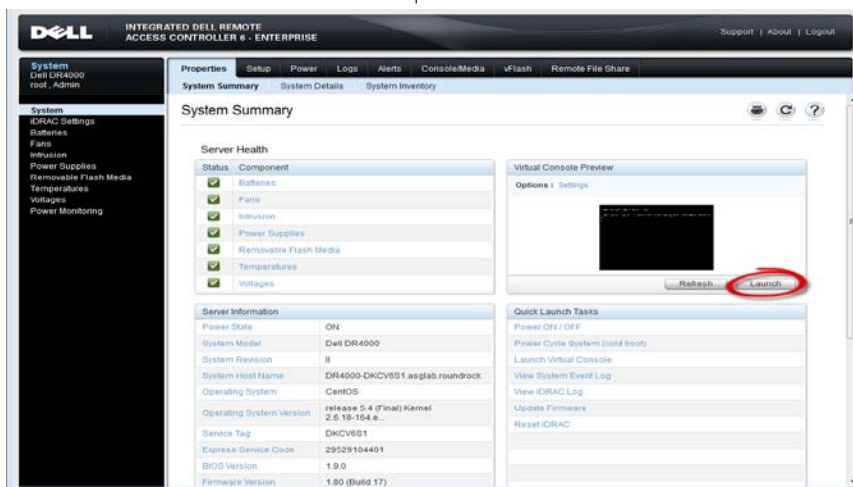
For additional data management application (DMA) best practice whitepapers, see the DR Series system documentation at <http://www.dell.com/support/Manuals/us/en/19/Product/powervault-dr4100>.

Note: The DR Series system and AppAssure screenshots used in this document may vary slightly, depending on the DR Series system firmware version and AppAssure version used.

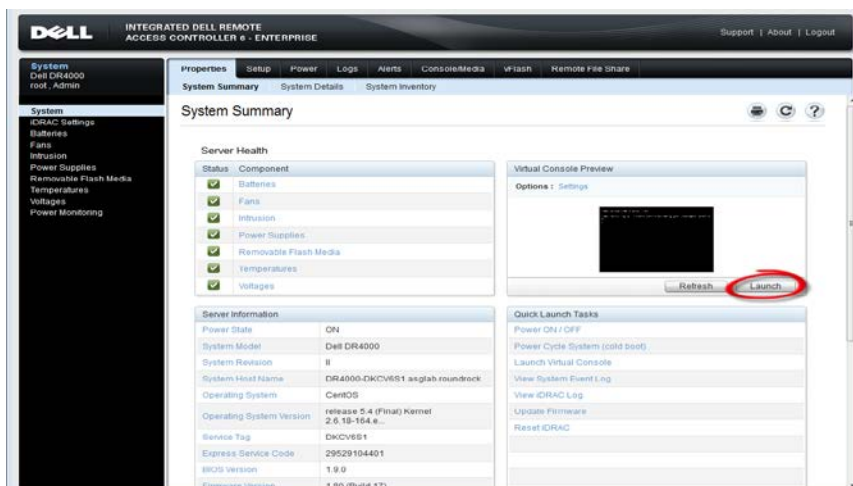


1 Install and configure the DR Series system

1. Rack and cable the DR Series system and power it on.
2. Initialize the DR Series system. Refer to the *Dell 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 in 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**".



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).

```
Ocarina release 1 (EAR-1.00.00) Build: 32858
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
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:
```

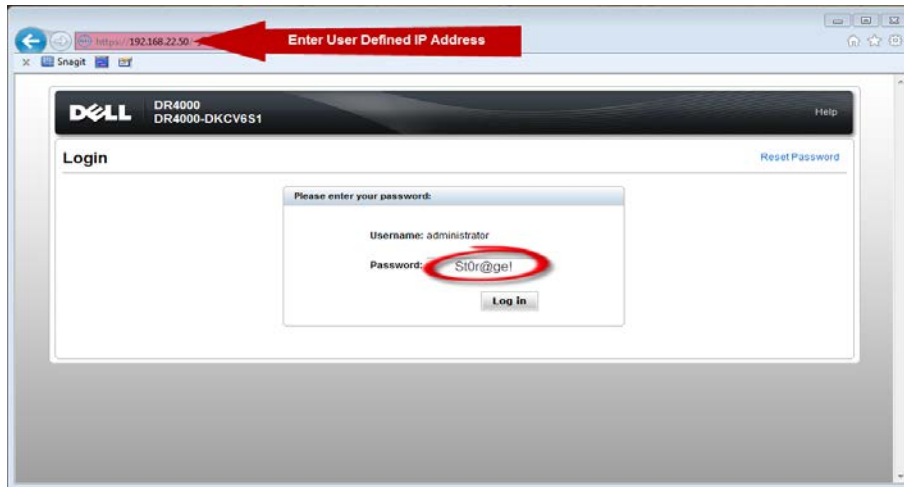
7. View the summary of preferences and confirm that it is correct.

```
=====
                          Set Static IP Address
IP Address      : 10.10.86.108
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       : DR4000-5

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



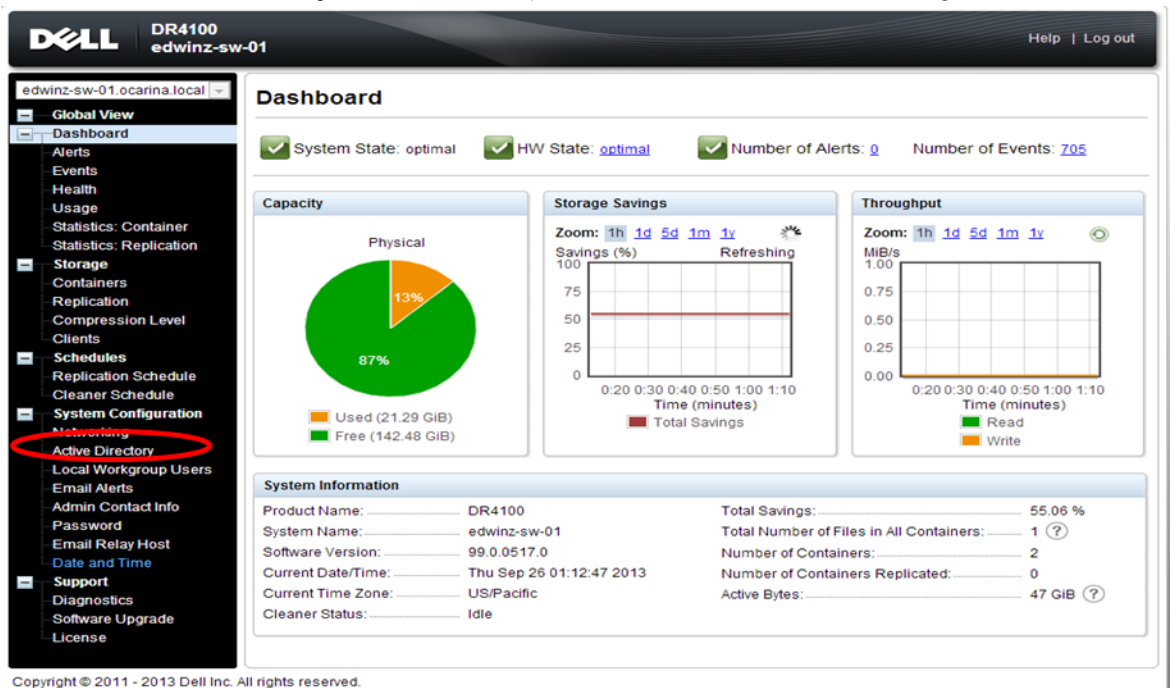
8. Log on to the DR Series system administrator console, using the IP address you just provided for the DR Series system and the username **administrator** and password **St0r@ge!** (the "0" in the password is the numeral zero).



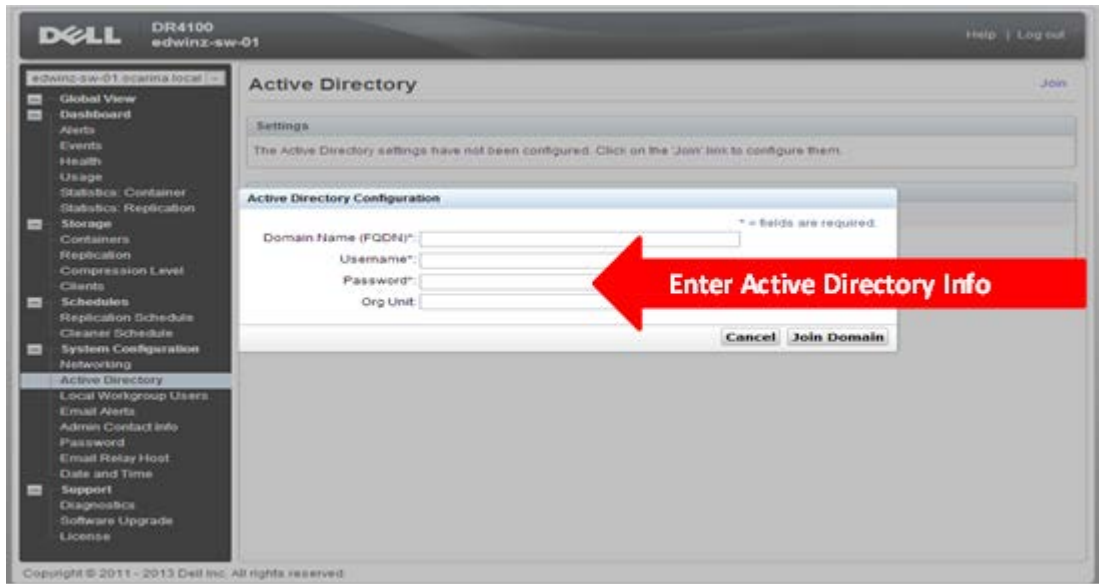
9. Join the DR Series system to Active Directory.

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.

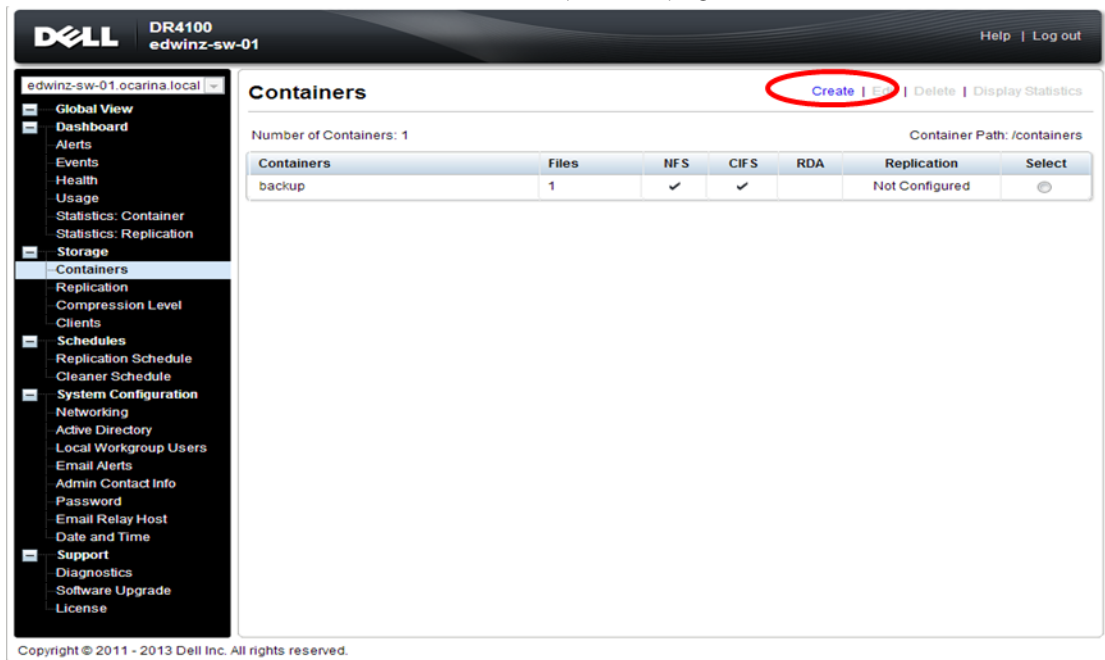
- a. Select **Active Directory** from the menu panel on the left side of the management interface.



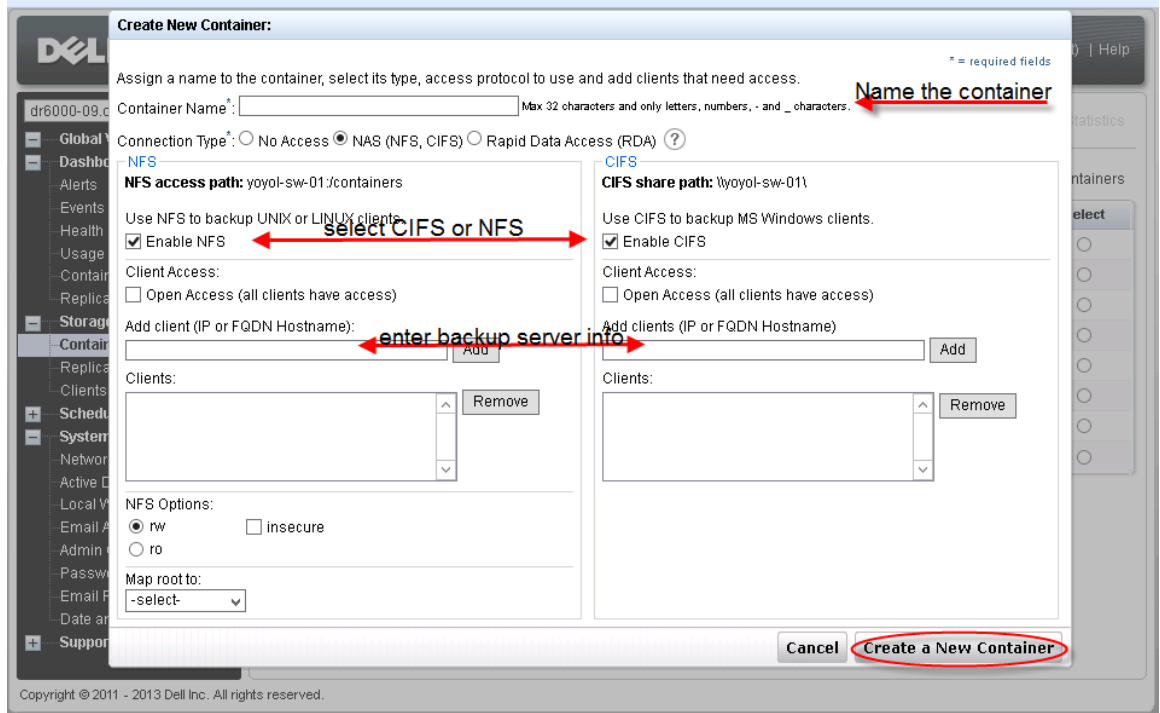
b. Enter your Active Directory credentials.



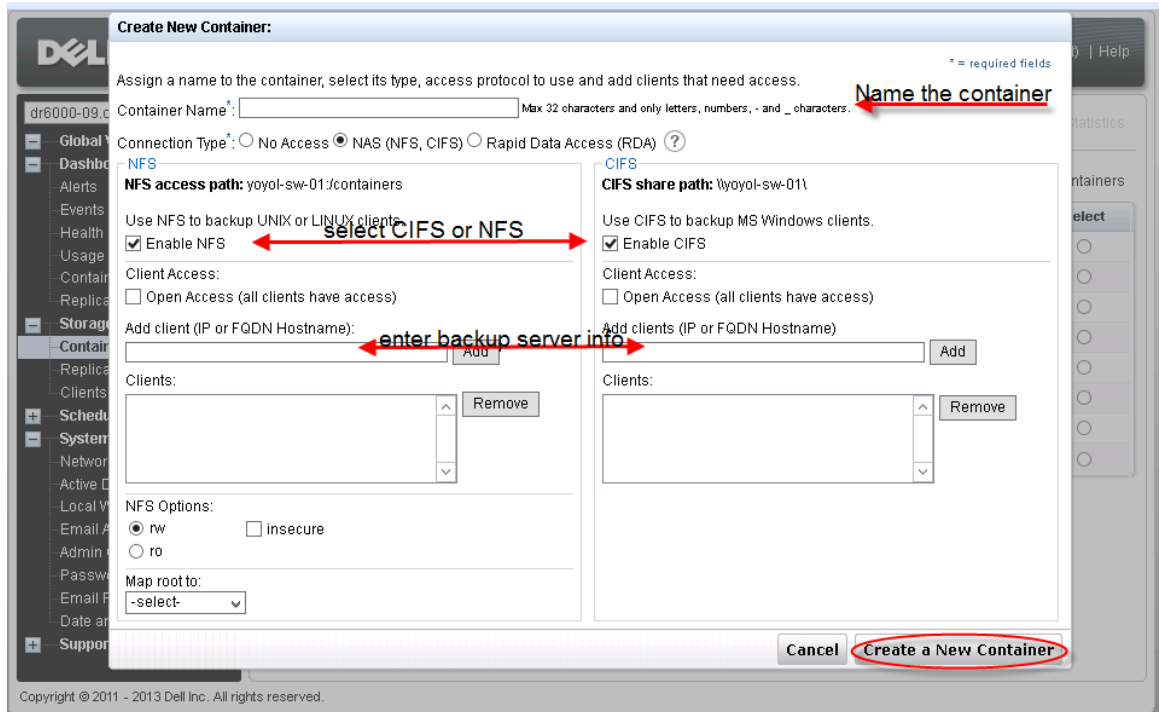
10. Create and mount the container. Select **Containers** in the navigation panel on the left side of the dashboard, and then click the **Create** at the top of the page.



11. Enter a **Container Name** and select the **Enable CIFS** checkbox. (AppAssure supports CIFS protocols.)



12. Select the preferred client access credentials.



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

13. Click **Create a New Container**. Confirm that the container has been added.

The screenshot shows the Dell DR6000 management console interface. The top navigation bar includes the Dell logo, 'DR6000', and user information 'administrator (Log out) | Help'. A left sidebar contains a navigation menu with categories like Global View, Dashboard, Alerts, Health, Usage, Container Statistics, Storage, Containers, Schedules, System Configuration, and Support. The main content area is titled 'Containers' and features a 'Message' box with a green checkmark icon and the following text:

- Successfully added container "AppAssure".
- Successfully added NFS connection for container "AppAssure".
- Successfully added CIFS connection for container "AppAssure".

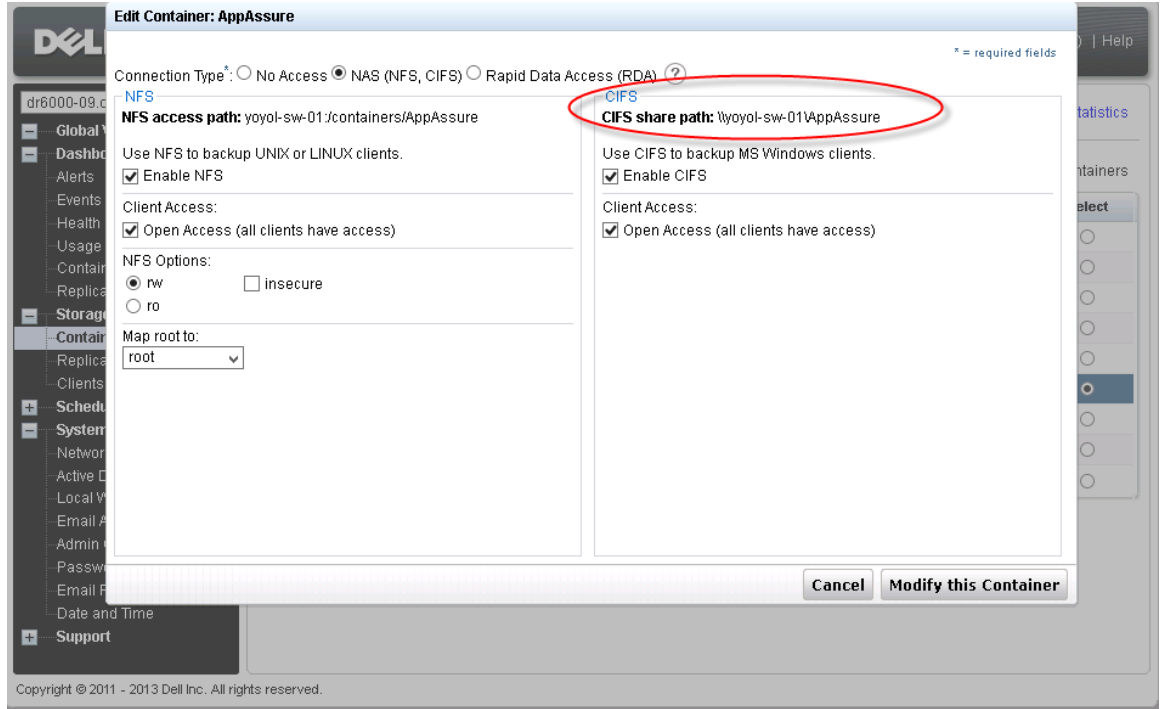
Below the message, it states 'Number of Containers: 9' and 'Container Path: /containers'. A table lists the containers with the following data:

Containers	Files	NFS	CIFS	RDA	Replication	Select
aa1	15		✓		Stopped	<input type="radio"/>
aa2	11		✓		Not Configured	<input type="radio"/>
aa3	11		✓		Not Configured	<input type="radio"/>
aa4	15		✓		Not Configured	<input type="radio"/>
aa5	7		✓		Not Configured	<input type="radio"/>
AppAssure	0	✓	✓		Not Configured	<input type="radio"/>
backup	0	✓	✓		Not Configured	<input type="radio"/>
rep1	4		✓		Not Configured	<input type="radio"/>
yy4	6		✓		Not Configured	<input type="radio"/>

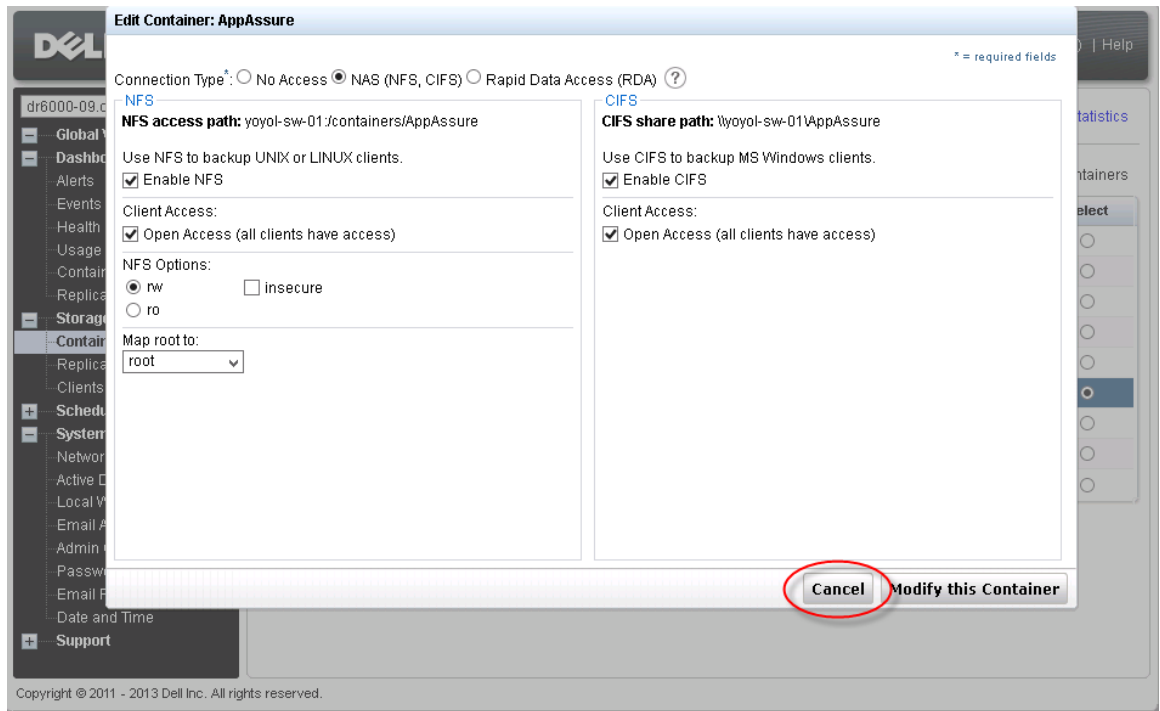
Copyright © 2011 - 2013 Dell Inc. All rights reserved.



14. Click **Edit**. Note the container share/export path, which you will use later to target the DR Series system.



15. To exit, click **Cancel**.



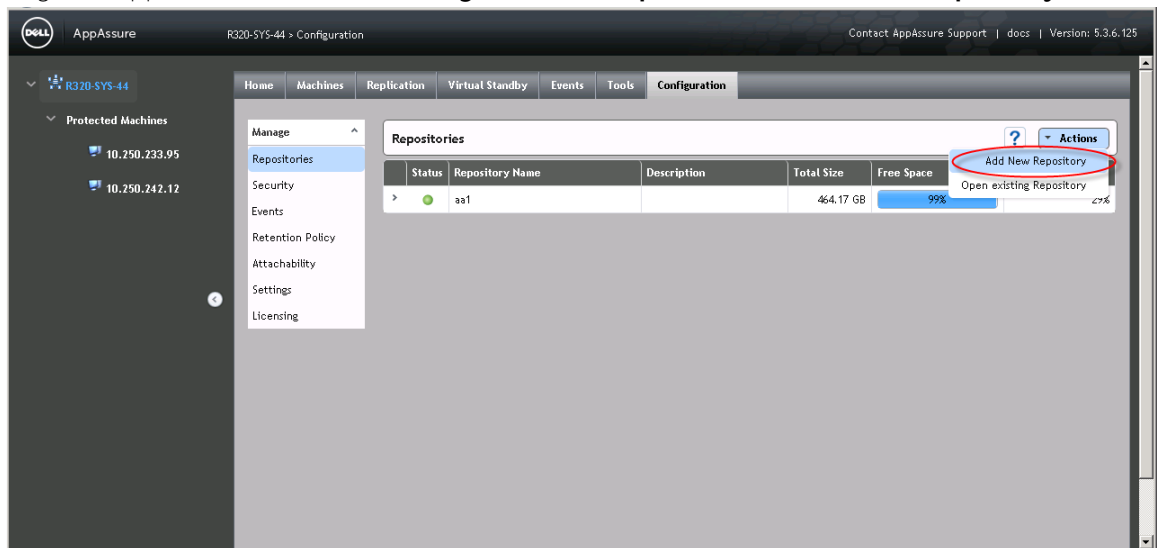
2 Set up AppAssure

2.1 Archive backup images to the DR Series system

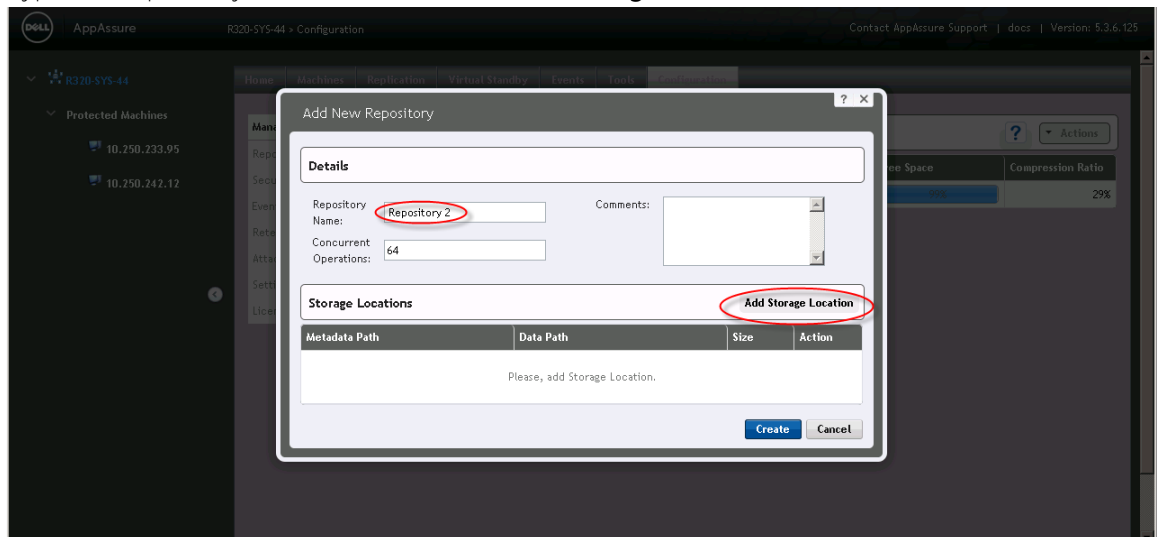
To create a backup job and back up a Windows data set, follow steps 1-8 in the procedure that follows. If you already have a backed up data set, skip steps 1-8 and start from step 9 to archive the backup data set to the DR Series system.

Note about Linux backup images: Steps 9-12 in the following procedure is for archiving both Windows and Linux backup images. To generate Linux backup images, see Appendix A.2.

1. Login to AppAssure Core. Click **Configuration -> Repositories -> Add New Repository**.



2. Type in a repository name and then click **Add Storage Location**.



- Enter the **Storage Location** details; the storage location is the target location for backup job. Click **Save**.

Add Storage Location

Storage Location

Add file on local disk
 Add file on CIFS share

Metadata Path:
UNC path:

Data Path:
User Name:

Password:

We recommend placing the repository in a dedicated folder (i.e. X:\Repository\). Placing the repository in the root (i.e. X:\) is not recommended as a delete of the repository will delete the entire contents of the repository path.

Details Show/Hide Details

Size:

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

Save **Cancel**

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

AppAssure YOYO-WIN2KBR2-0 Home Contact AppAssure Support | doc | Version: 5.3.6.12

YOYO-WIN2KBR2-0

Protected Machines Protect Machine Protect Cluster

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
●	10.30.149.74	Repository 1	11/27/2013 12:01:57 PM	8	992.6 MB

Repositories Add New Repository

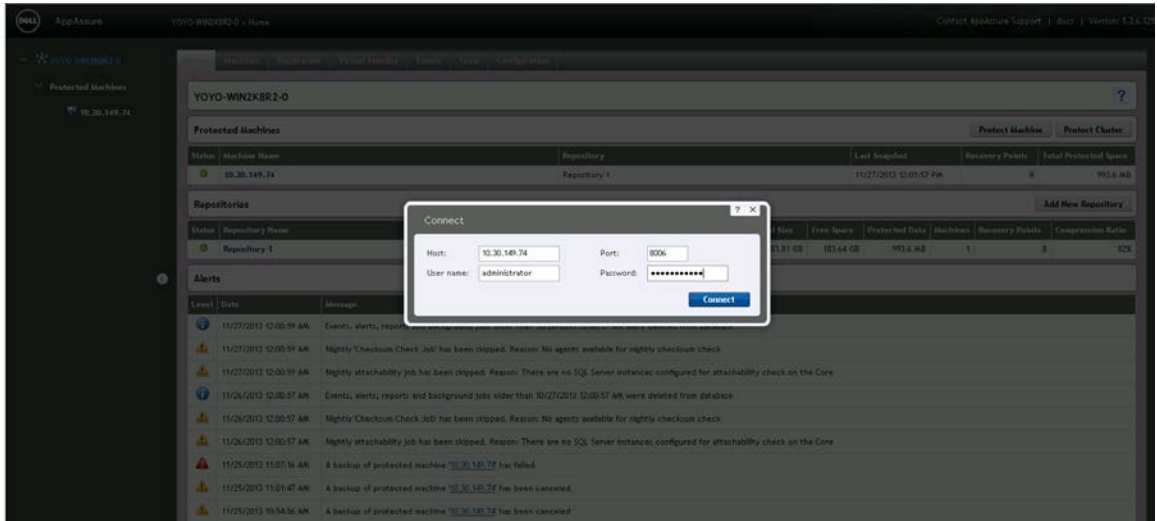
Status	Repository Name	Total Size	Free Space	Protected Data	Machines	Recovery Points	Compression Ratio
●	Repository 1	183.81 GB	183.64 GB	992.6 MB	1	8	82%

Alerts

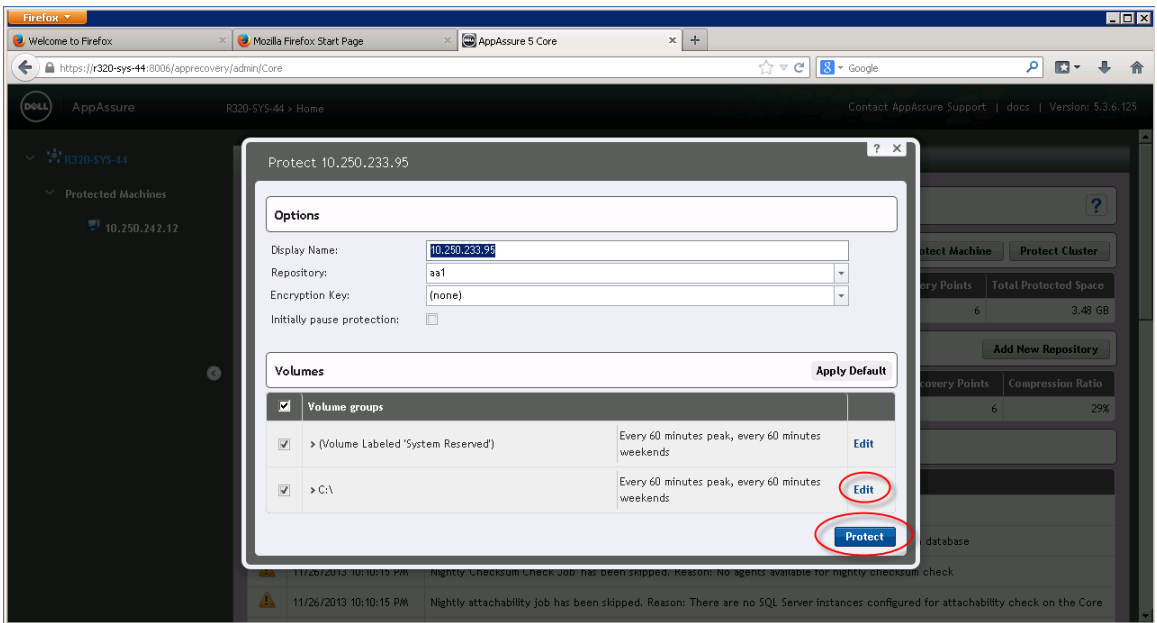
Level	Date	Message
i	11/27/2013 12:00:59 AM	Events, alerts, reports and background jobs older than 10/28/2013 12:00:59 AM were deleted from database
!	11/27/2013 12:00:59 AM	Nightly 'Checksum Check Job' has been skipped. Reason: No agents available for nightly checksum check.
i	11/27/2013 12:00:59 AM	Nightly attachability job has been skipped. Reason: There are no SQL Server instances configured for attachability check on the Core.
i	11/26/2013 12:00:57 AM	Events, alerts, reports and background jobs older than 10/27/2013 12:00:57 AM were deleted from database
!	11/26/2013 12:00:57 AM	Nightly 'Checksum Check Job' has been skipped. Reason: No agents available for nightly checksum check.
!	11/26/2013 12:00:57 AM	Nightly attachability job has been skipped. Reason: There are no SQL Server instances configured for attachability check on the Core.
!	11/25/2013 11:07:16 AM	A backup of protected machine '10.30.149.74' has failed.
!	11/25/2013 11:01:47 AM	A backup of protected machine '10.30.149.74' has been canceled.
!	11/25/2013 10:54:56 AM	A backup of protected machine '10.30.149.74' has been canceled.



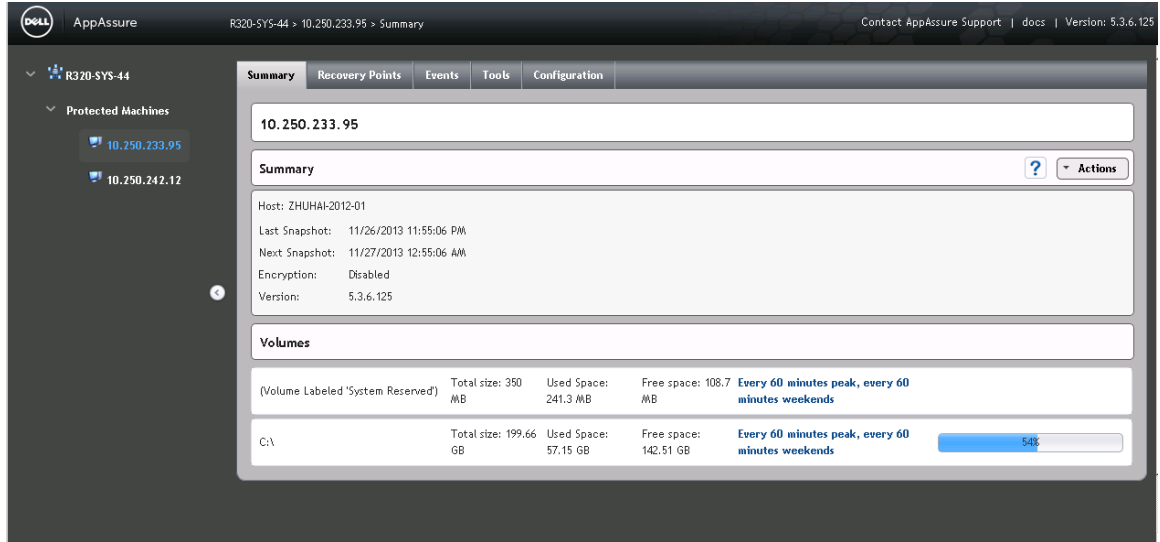
5. Enter the client machine information and click **Connect**.



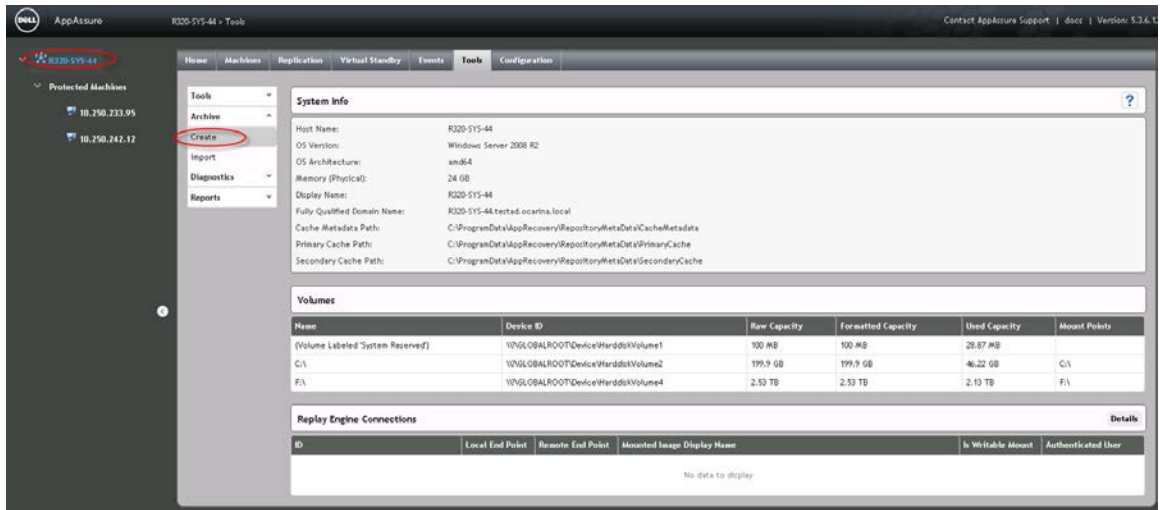
6. Check or uncheck each volume group to select the backup data set. To change backup schedules, click **Edit**. Click **Protect**.



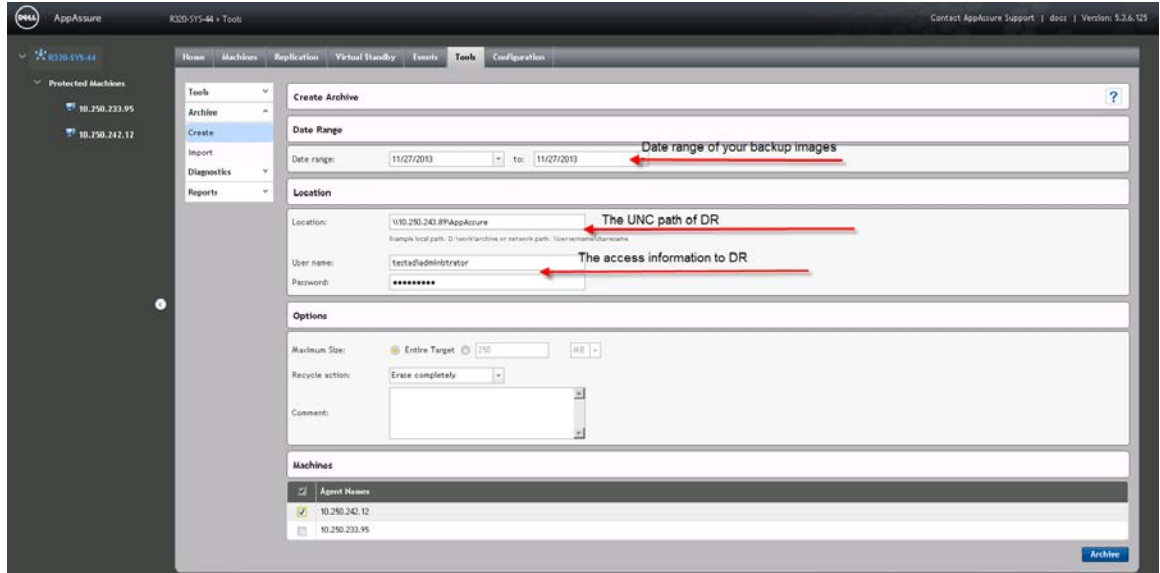
- The machines that have been protected by AppAssure are listed on the left side under **Protected Machines**.



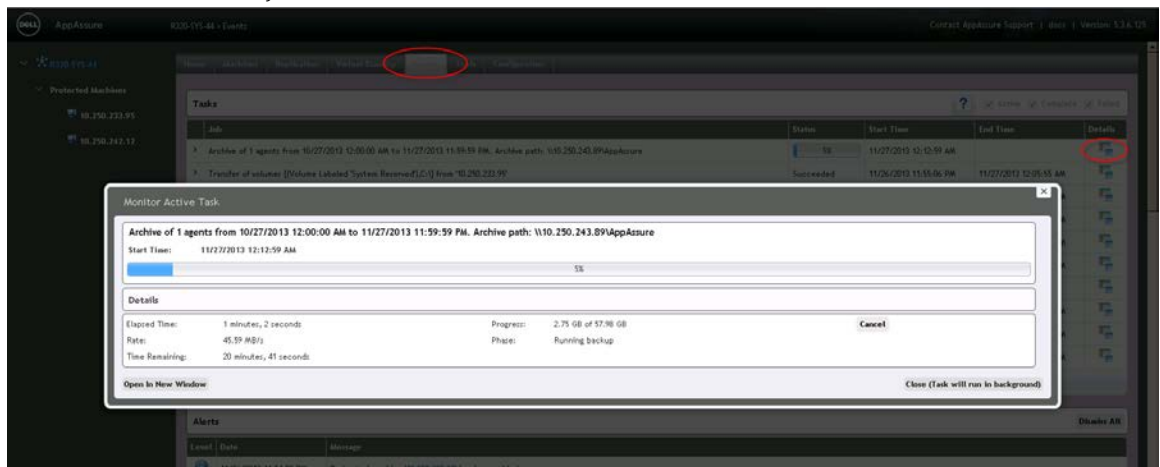
- AppAssure creates backup images for the protected machines according to the protection policy. To see the backup images, click **Protected Machines -> Recovery Points**.



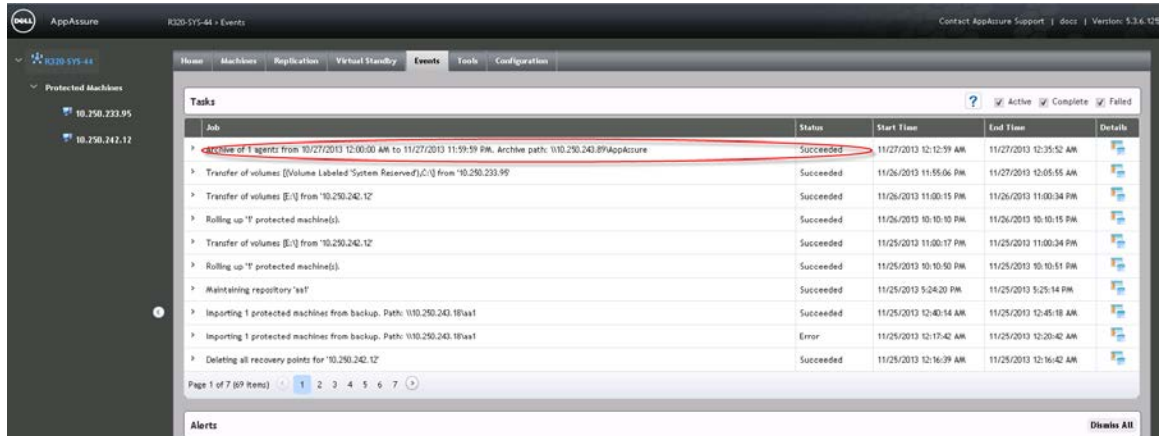
- To create an archive job, click **Core Server** -> **Tools** -> **Archive** -> **Create**. Enter all of the required information then click **Archive**.



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



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

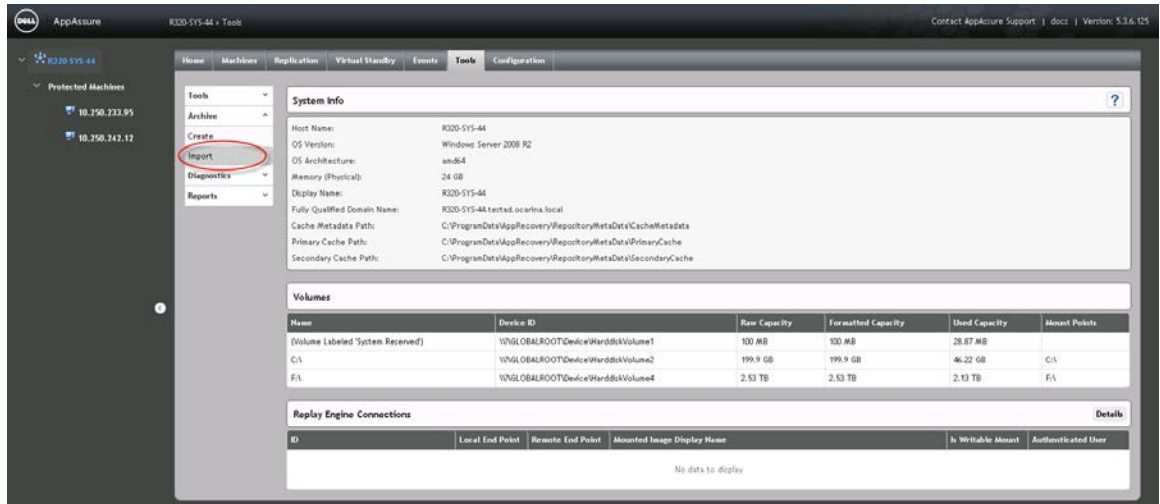


12. To return to the **Next Step Wizard** page, click **Finish**. To close the window, click **Close**.

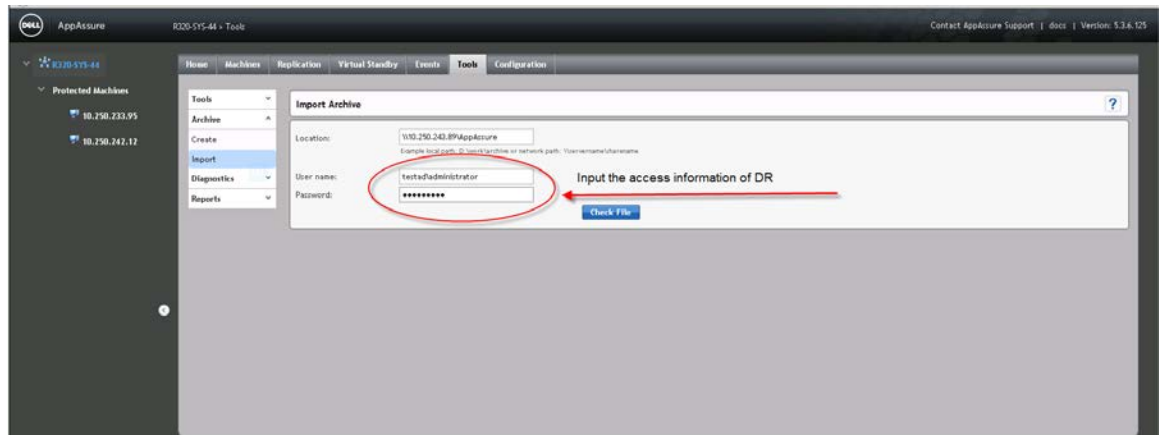


2.2 Restore archived backup images from the DR Series system

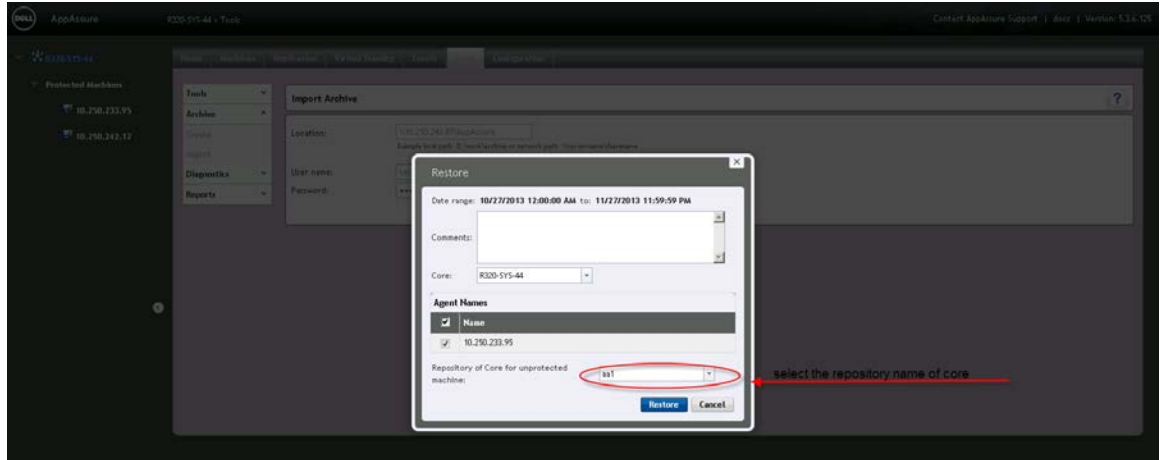
1. Click **Tools** -> **Archive** -> **Import**.



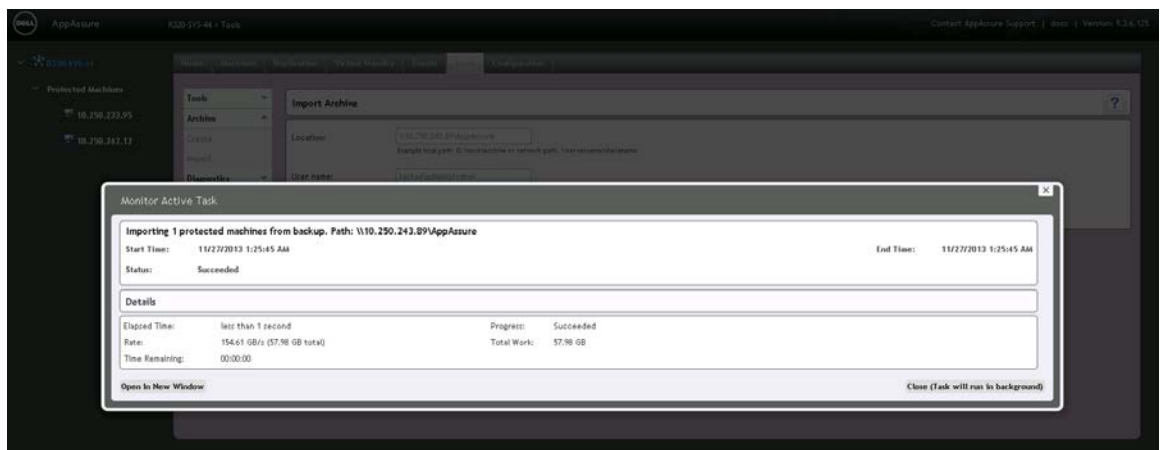
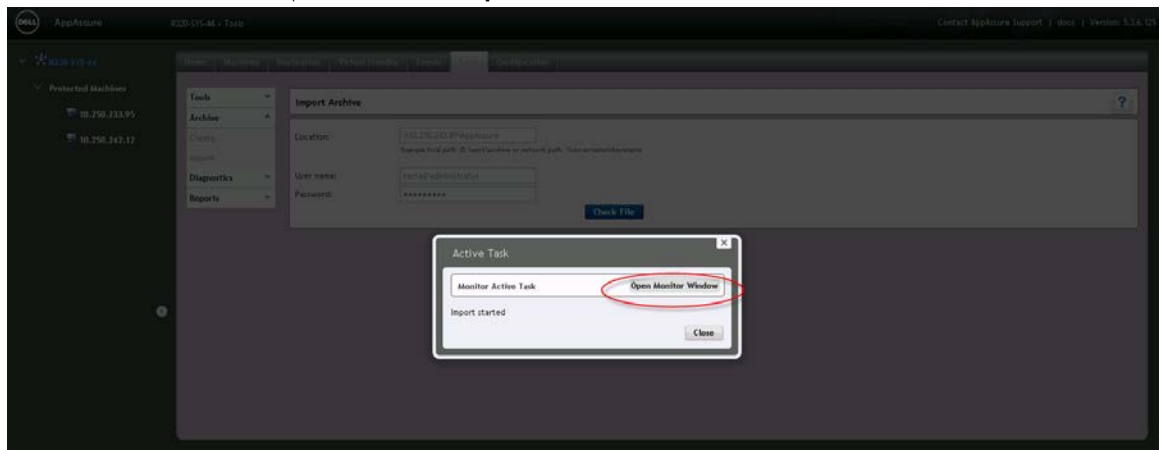
2. Enter the UNC path of the DR container share that holds the archive images. In addition, enter the CIFS credentials for authenticating to the DR Series system. Click **Check File**.



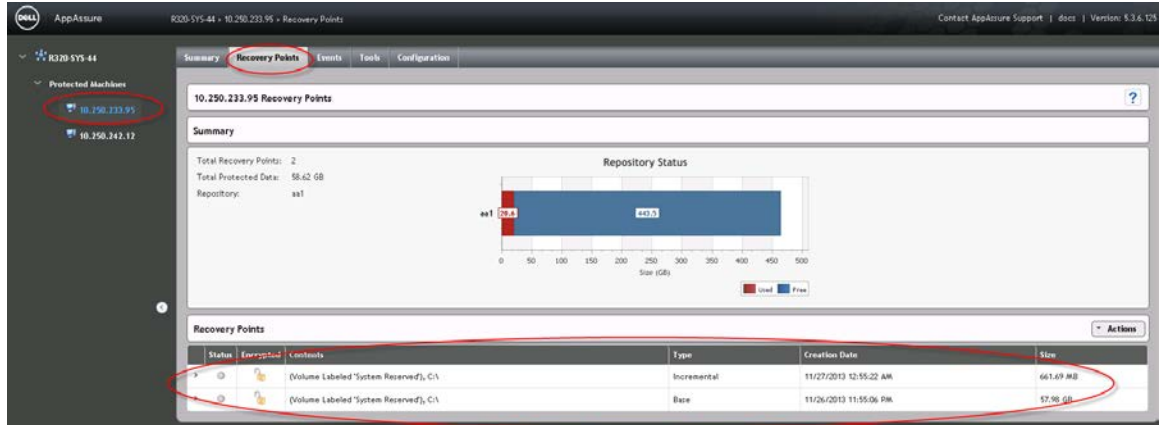
- Under **Agent Names**, select the agent and repository that the archived data will be imported to and click **Restore**.



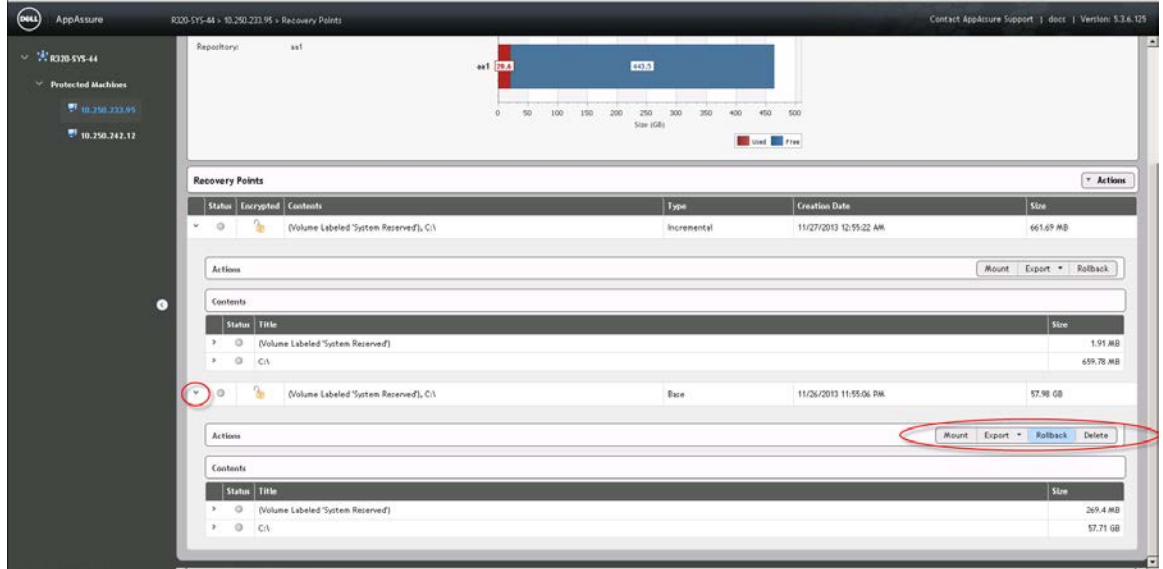
- To monitor the restore process, click **Open Monitor Window**.



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



- Each of the recovery points can be expanded to show available operations.



3 Set 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 shown in the following screenshot 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 six hours per week when backups are not taking place, and generally after a backup job has completed.

The screenshot shows the Dell DR Series system cleaner configuration interface. The sidebar menu on the left includes sections for Dashboard, Alerts, Events, Health, Usage, Statistics: Container, Statistics: Replication, Storage, Containers, Replication, Compression Level, Clients, Schedules, Replication Schedule, Cleaner Schedule (highlighted), System Configuration, Networking, Active Directory, Local Workgroup Users, Email Alerts, Admin Contact Info, Password, Email Relay Host, Date and Time, Support, Diagnostics, Software Upgrade, and License. The main content area is titled 'Cleaner Schedule' and displays the following information:

System time zone: US/Pacific, Fri Jul 5 05:00:41 2013

Note: When no schedule is set, the cleaner will run as needed.

Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--

An 'Edit Schedule' button is visible in the top right corner, and a red arrow points to it with the text 'Schedule Cleaner'.

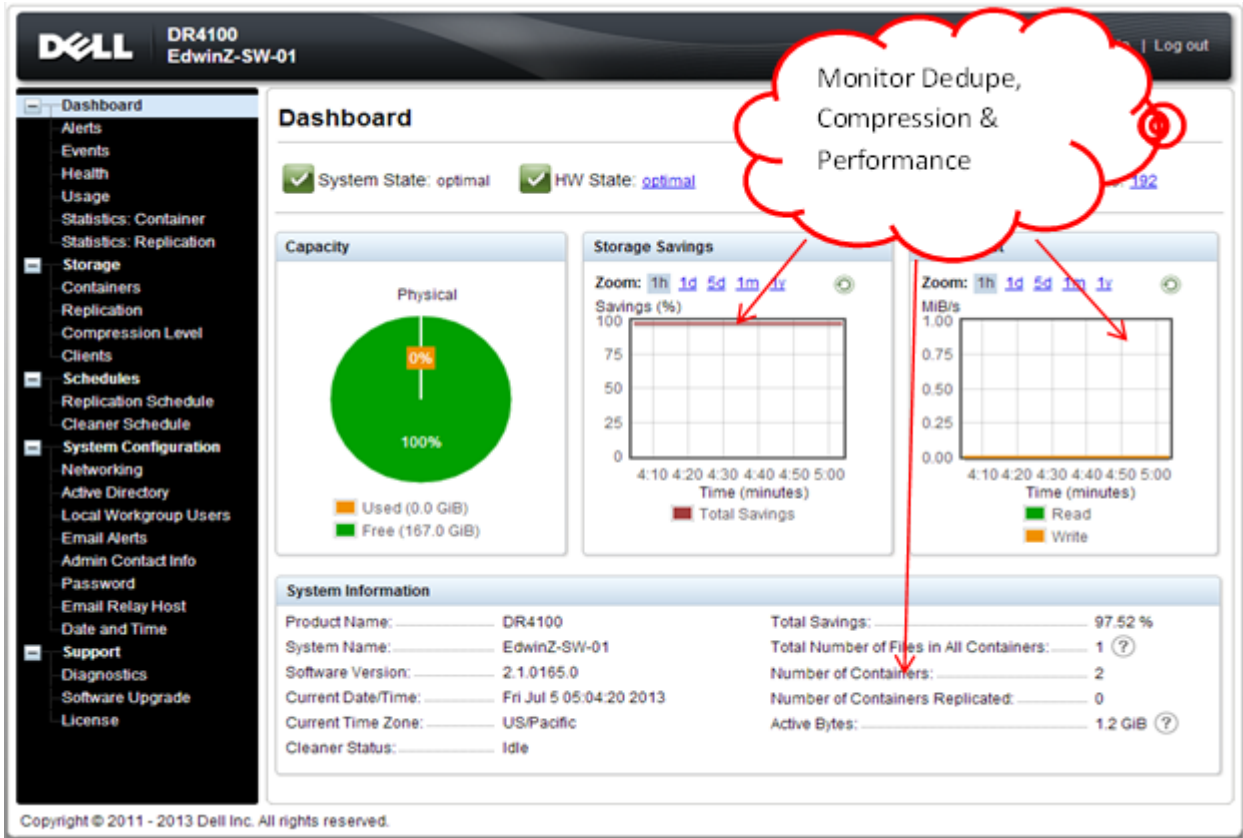
Copyright © 2011 - 2013 Dell Inc. All rights reserved.



4 Monitor 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.

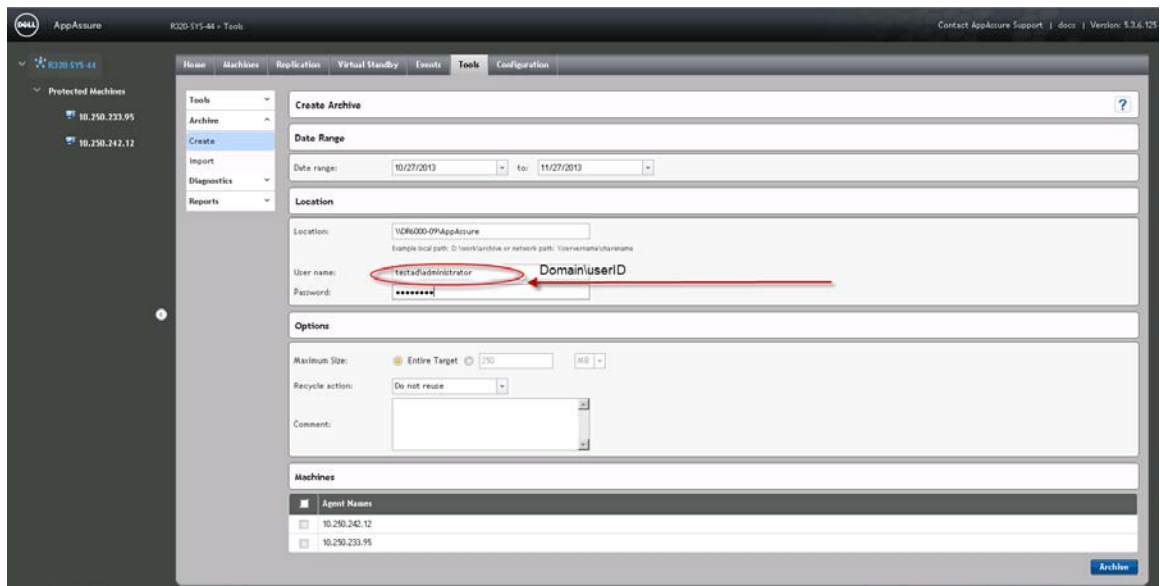


A Appendix

A.1 Configure the DR container share as a CIFS storage device on AppAssure

In order to configure the DR container share as an archive destination, AppAssure needs to authenticate to a DR Series system.

- If DR is joined into an Active Directory domain, you must enter **[domain_name]\user_id** in the **User Name** field for successful authentication.



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



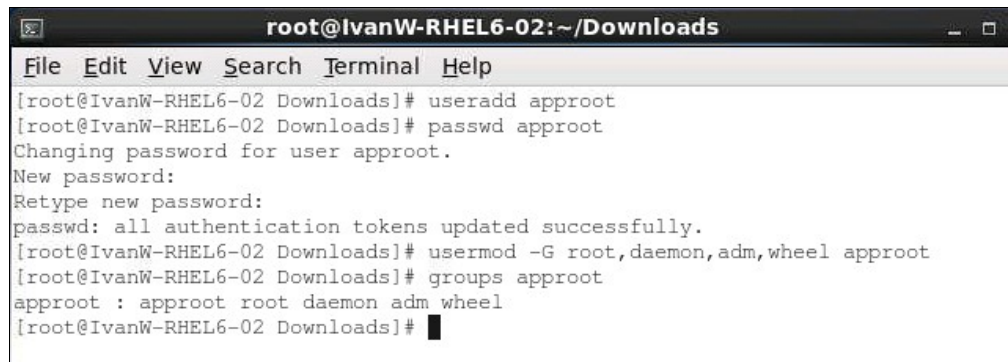
A.2 Back up a Linux client

A.2.1 Install the Linux agent onto the client machine

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

On the Linux client machine, run the commands below as the **root** user:

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_5.3.6.125.sh`

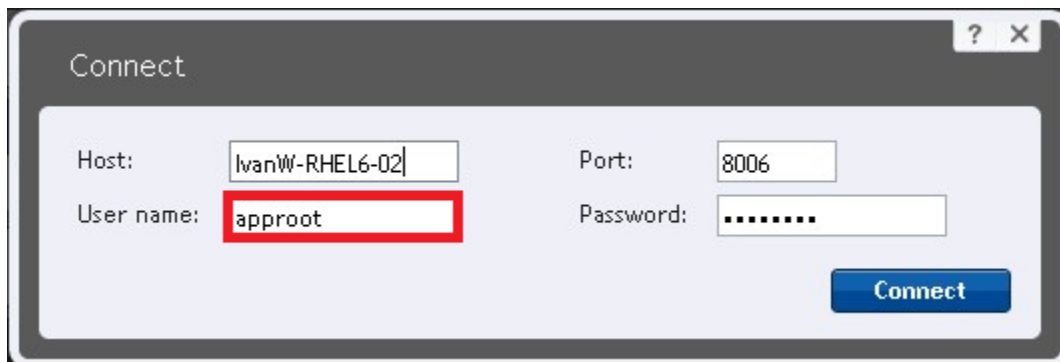



```
root@IvanW-RHEL6-02:~/Downloads
File Edit View Search Terminal Help
tar: appassure-packages/appassure-agent-5.3.6-125el6.x86_64.rpm: time stamp 2013-11-03 16:45:17 is 1149951.791499555 s in the future
tar: appassure-packages/version: time stamp 2013-11-03 16:46:03 is 1149997.790834578 s in the future
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/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]:
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>.

A.2.2 Back up the Linux client machine

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



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



2. In the **Protect** dialog box, edit the settings as needed, and then click **Protect**.

Protect IvanW-RHEL6-02

Options

Display Name: IvanW-RHEL6-02

Repository: rep01

Encryption Key: (none)

Initially pause protection:

Volumes Apply Default

<input checked="" type="checkbox"/>	Volume groups		
<input checked="" type="checkbox"/>	> /	Every 60 minutes peak, every 60 minutes weekends	Edit
<input checked="" type="checkbox"/>	> /boot	Every 60 minutes peak, every 60 minutes weekends	Edit

Protect

