Setting Up the Dell™ DR Series System as an Archive Target on AppAssure 5.4.3

Dell Engineering
April 2015

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release
April 2015	Updated for DR Series system 3.2 software release

Table of contents

Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for AppAssure 5.4.3.

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://www.dell.com/powervaultmanuals

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   Installing and configuring the DR Series system

1. Rack and cable the DR Series system and power it on.

2. Initialize the DR Series system. For more information about this step, in the *Dell DR Series System Administrator Guide,* refer to 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 address assigned to the iDRAC interface. Use the user name and password: "**root/calvin**".
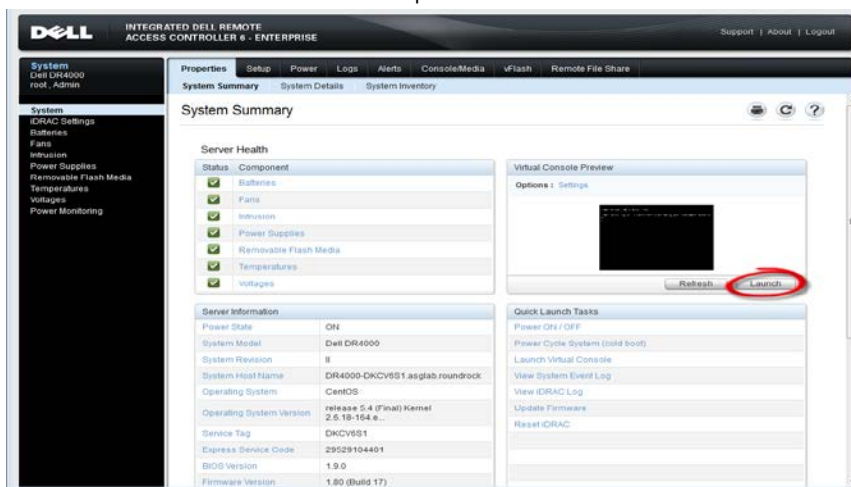
4. Launch the virtual console.
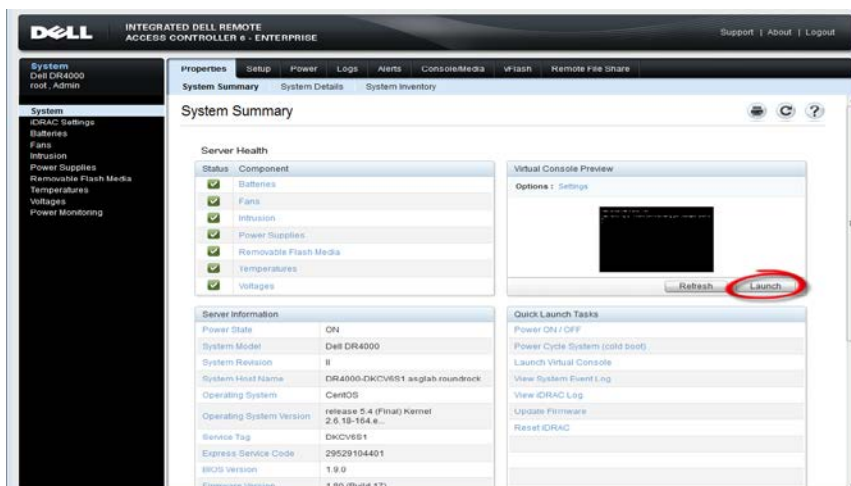
5. After the virtual console is open, log on to the system as user: **administrator** with the password: **St0r@ge!** (the "0" in the password is the numeral zero).

```
Ocarina release 1 (EAR-1.00.00) Build: 32050
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 with the username: **administrator** and password: **St0r@ge!** (the "0" in the password is the numeral zero.).
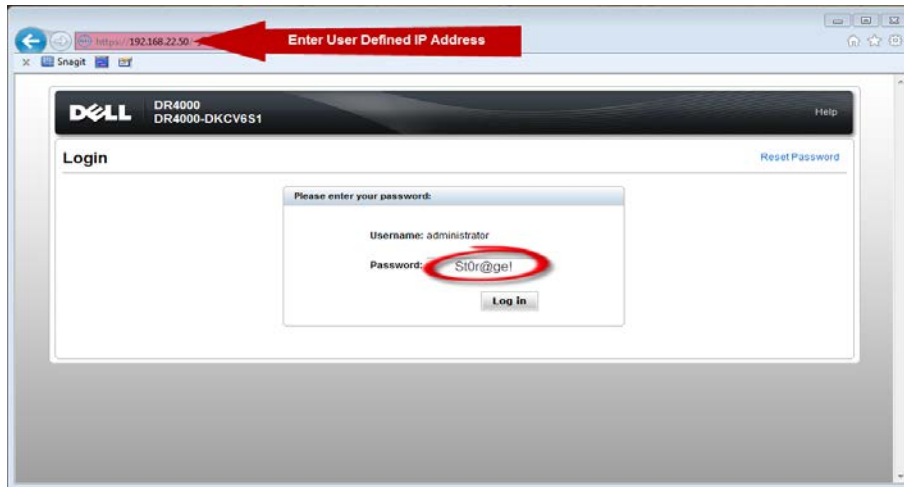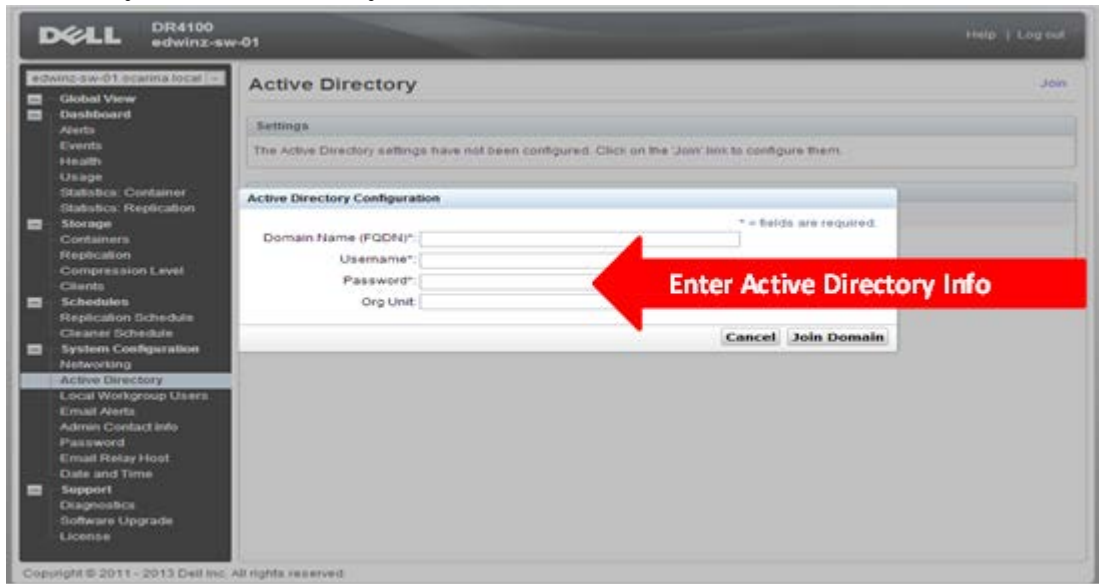

9. Join the DR Series system to Active Directory.

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 logon instructions.
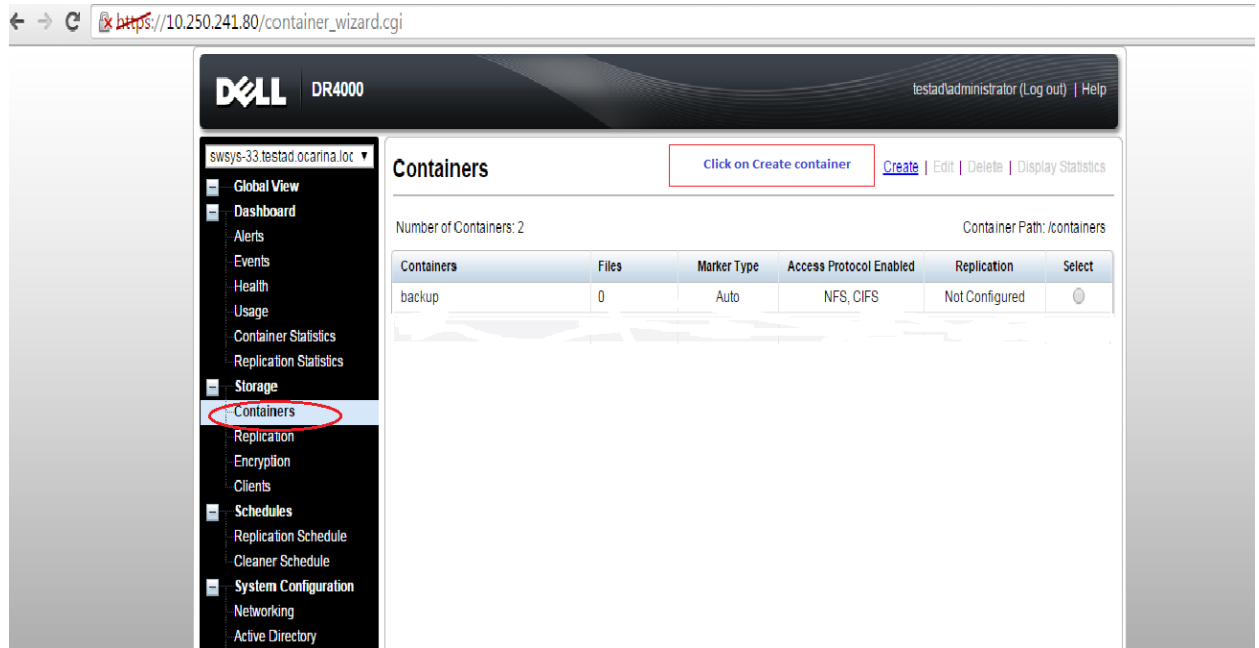
a. Select **Active Directory** from the navigation menu in the left side of the user interface.
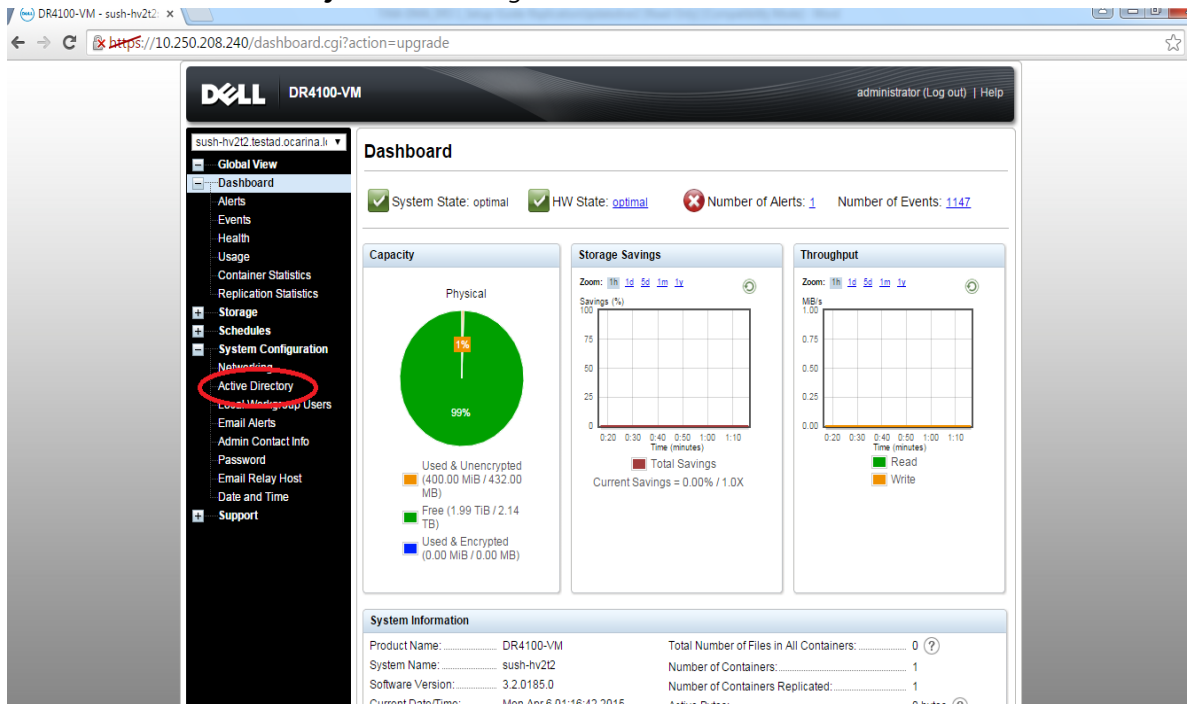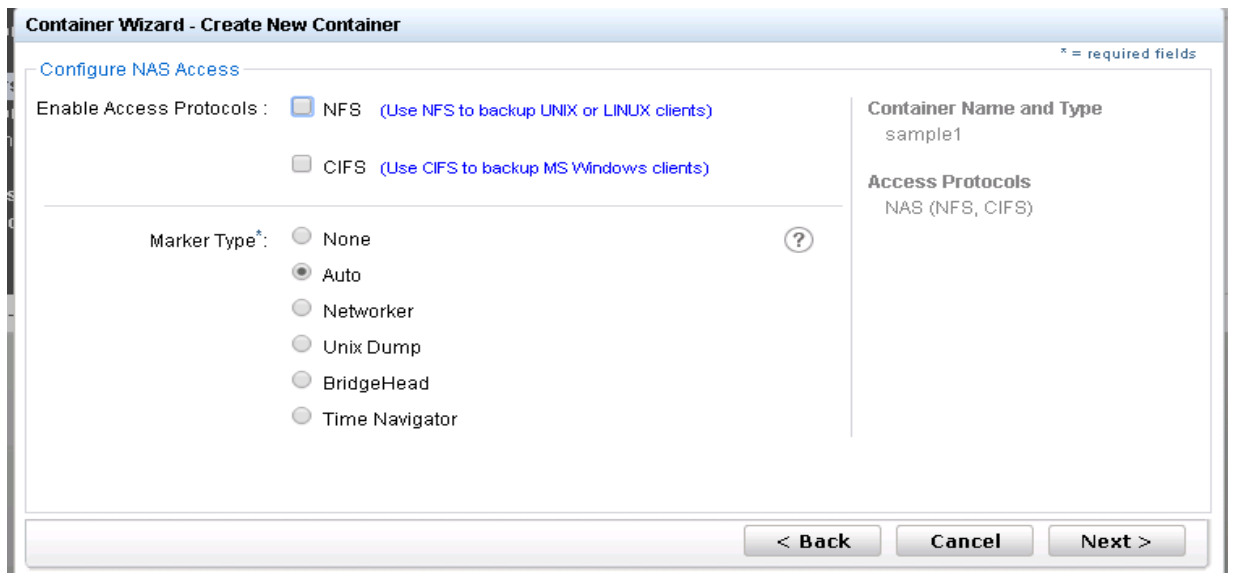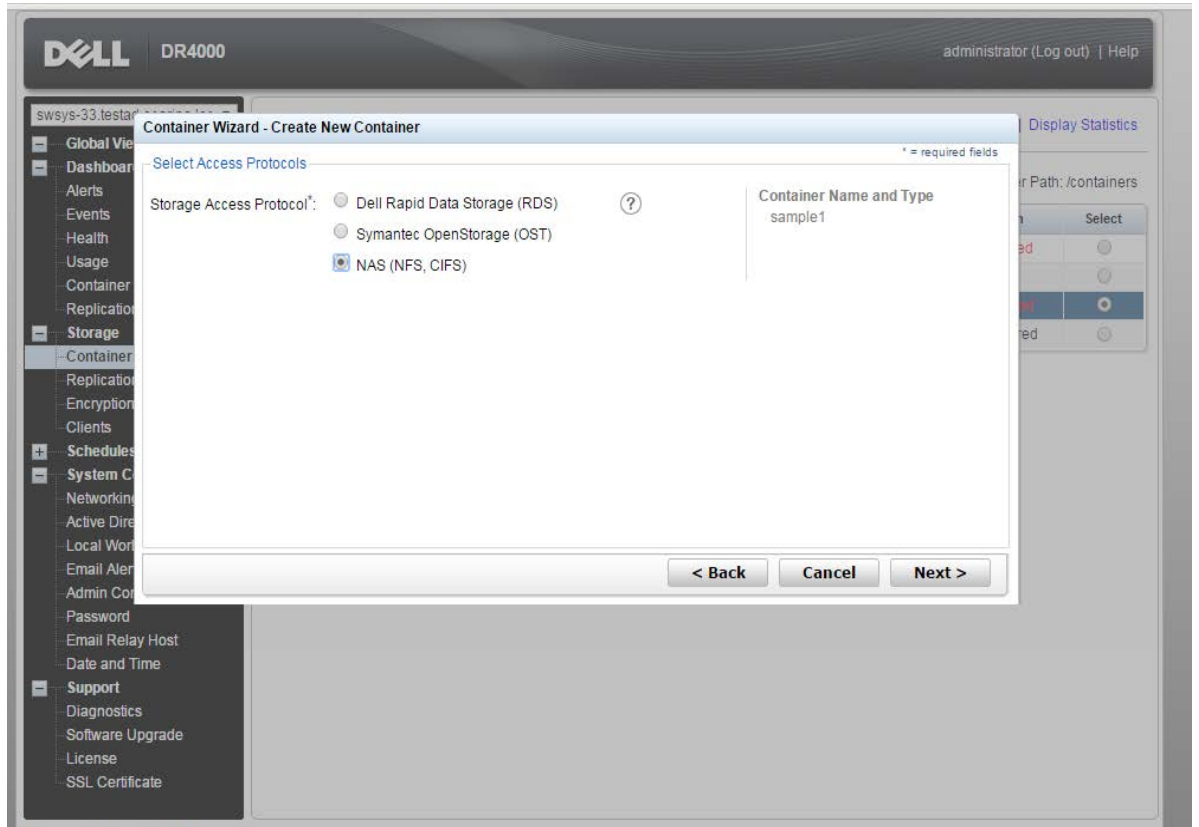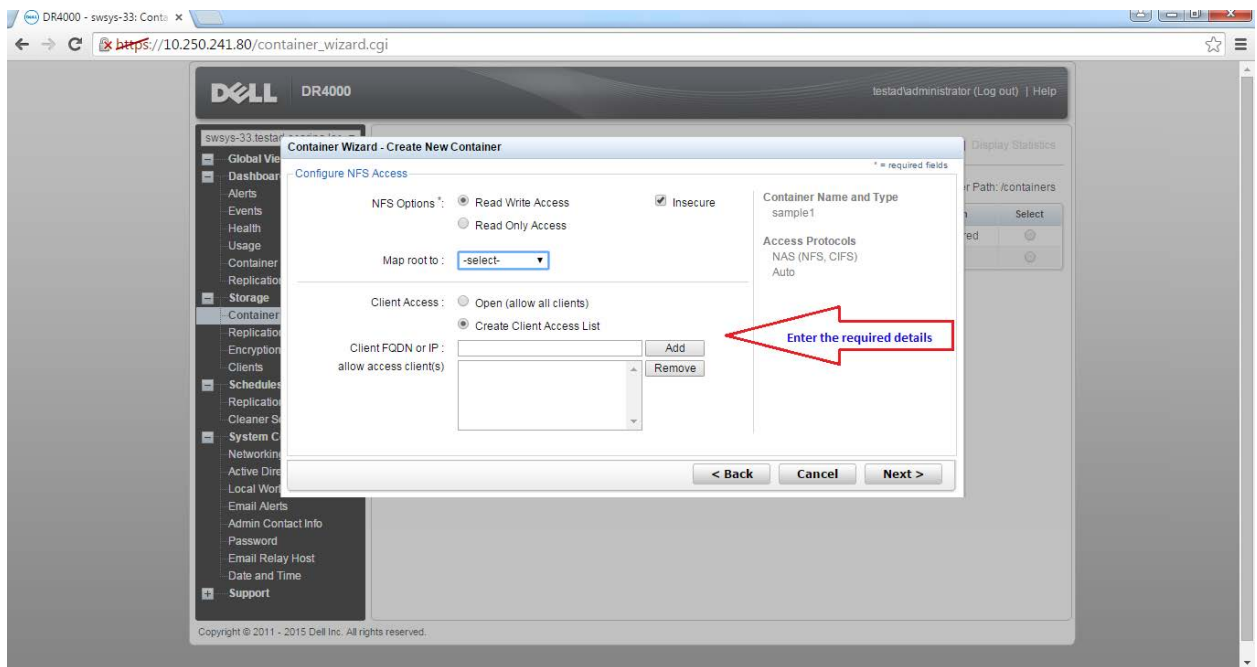
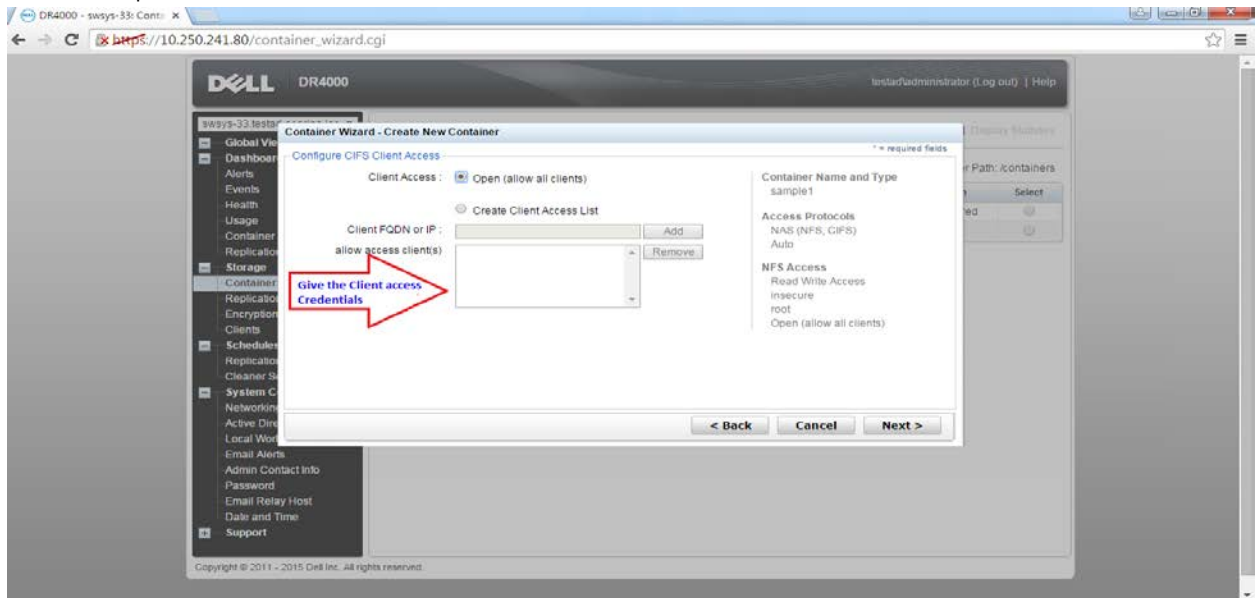b. Enter your Active Directory credentials.

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

11. Enter a **Container Name** and select the **Enable CIFS** checkbox. (AppAssure supports CIFS protocols.)
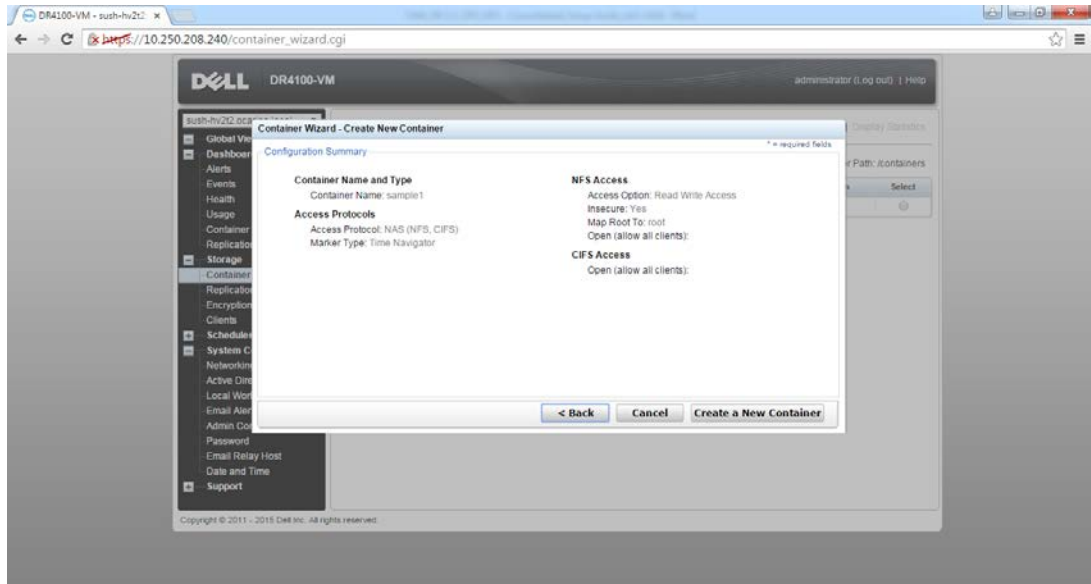
12. Select the preferred client access credentials.

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**, and then confirm that the container has been added.

14. Select the container, and click the **Display Statistics** link. Make a note of the container share/export path, which you will use later to target the DR Series system.

Container Name: sample1 ▼

Backup Data

Zoom: 1h 1d 5d 1m 1y

Num of Files

| 1.00 |
| 0.75 |
| 0.50 |
| 0.25 |
| 0.00 |

2:10 2:20 2:30 2:40 2:50 3:00
Time (hours)

■ Active Files

Zoom: 1h 1d 5d 1m 1y

Bytes

| 1.00 |
| 0.75 |
| 0.50 |
| 0.25 |
| 0.00 |

2:10 2:20 2:30 2:40 2:50 3:00
Time (minutes)

■ Active Bytes (?)

Throughput

Zoom: 1h 1d 5d 1m 1y

MiB/s

| 1.00 |
| 0.75 |
| 0.50 |
| 0.25 |
| 0.00 |

2:10 2:20 2:30 2:40 2:50 3:00
Time (hours)

■ Read
■ Write

* System Time Zone: US/Pacific

Marker Type: Auto　　　　**Connection Type: NFS / CIFS**

NFS Connection Configuration

NFS access path:	satyan-sw-02.ocarina.local:/containers/sample1
Client Access:	Open Access (all clients have access)
NFS Options:	rw,insecure
Map root to:	root
NFS Write Accelerator:	inactive

CIFS Connection Configuration

| CIFS share path: | \\satyan-sw-02.ocarina.local\sample1 |
| Client Access: | Open Access (all clients have access) |
| CIFS Write Accelerator: | inactive |

2 Setting up AppAssure

## 2.1 Archiving 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 are for archiving both Windows and Linux backup images. To generate Linux backup images, see Appendix A.2.

1. Log on to the AppAssure Core. Click **Configuration -> Repositories -> Add New Repository**.
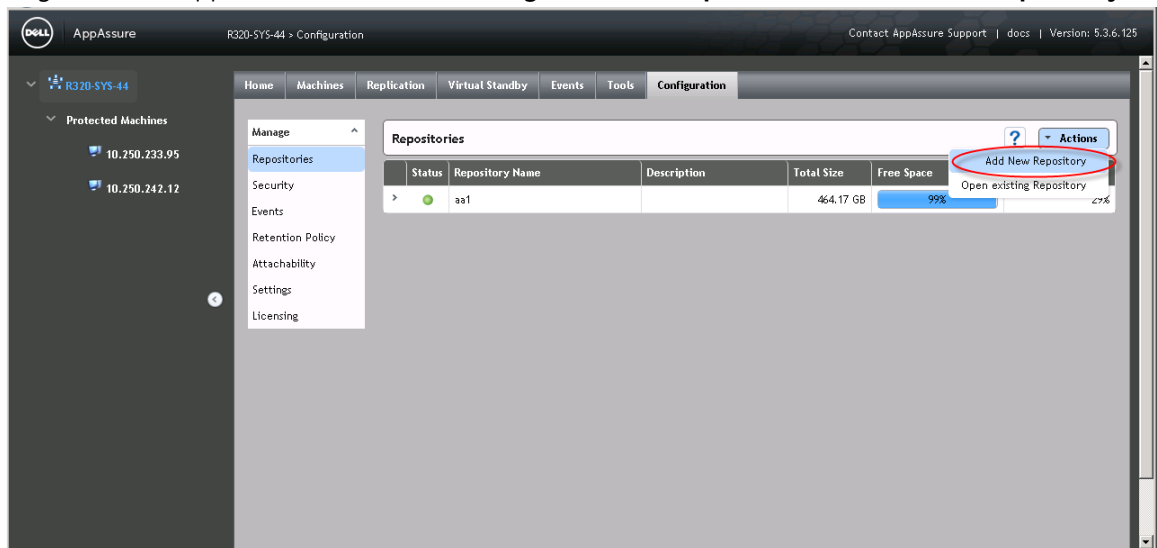
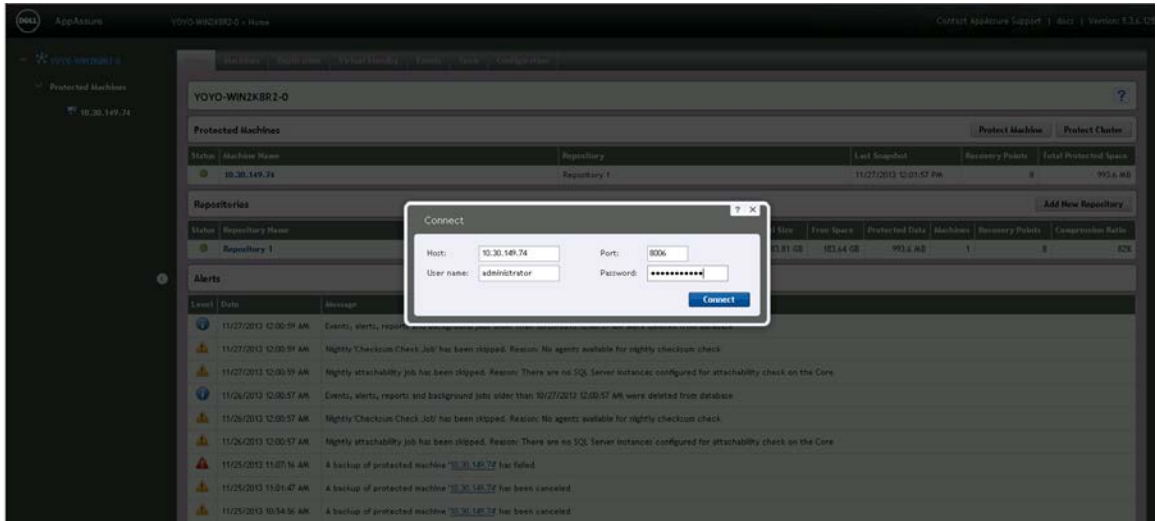2. Type in a repository name and then click **Add Storage Location.**
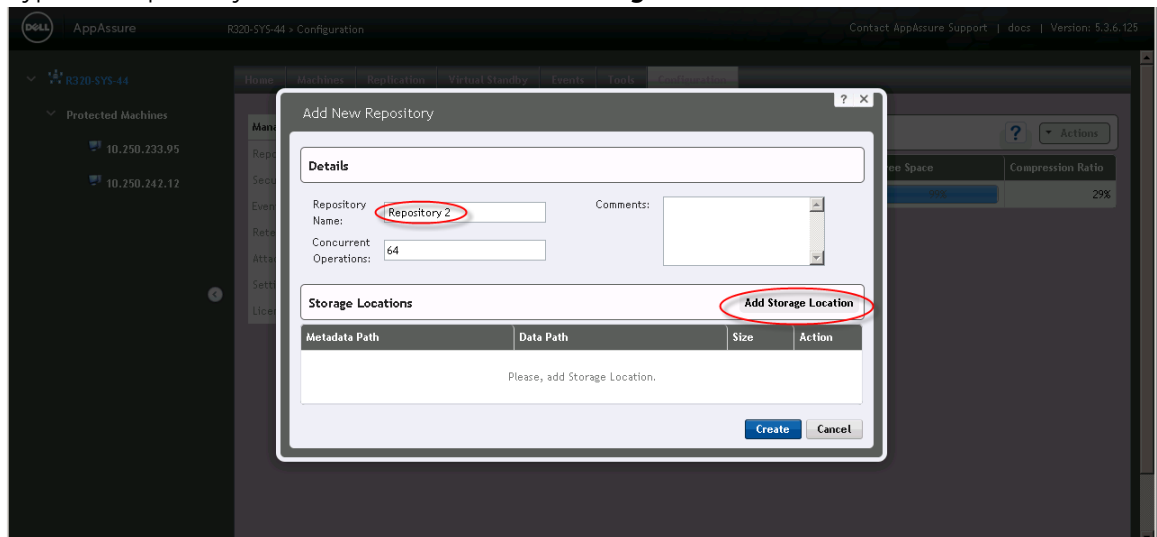
3. Enter the **Storage Location** details. (The storage location is the target location for backup job.) Click **Save**.
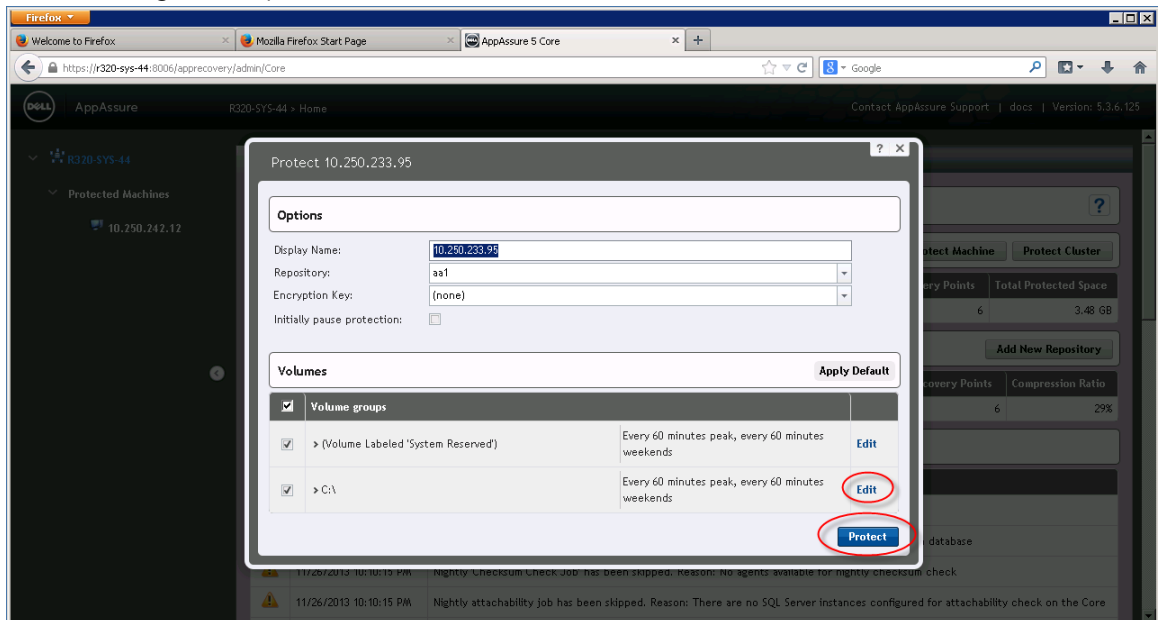

4. In the AppAssure core console, click **Home -> Protect Machine**.

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

6. Select or clear the checkbox for each volume group as needed to select the proper backup data set. To change backup schedules, click **Edit.** Click **Protect**.

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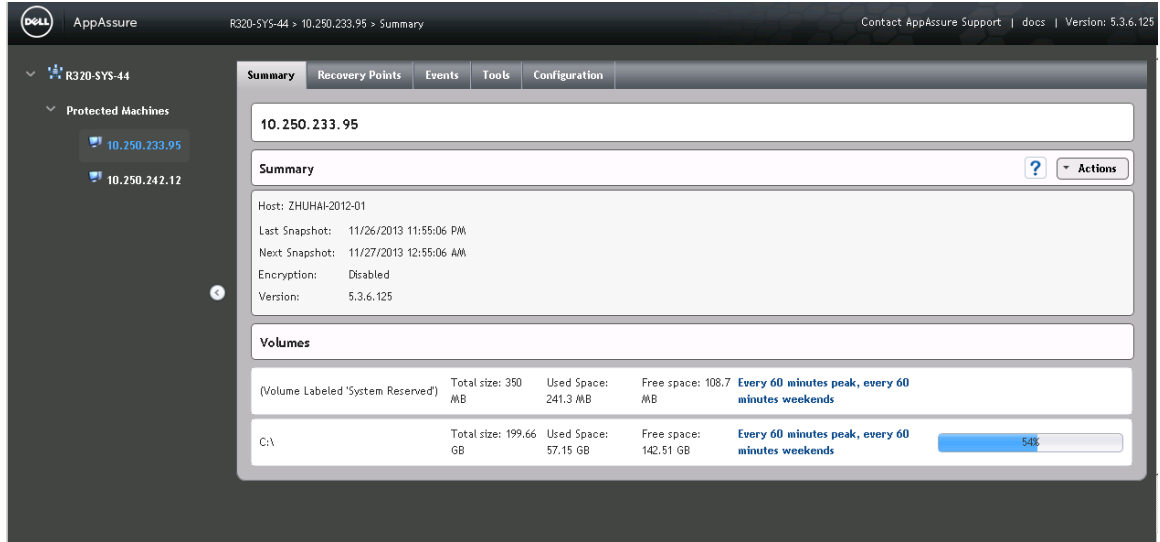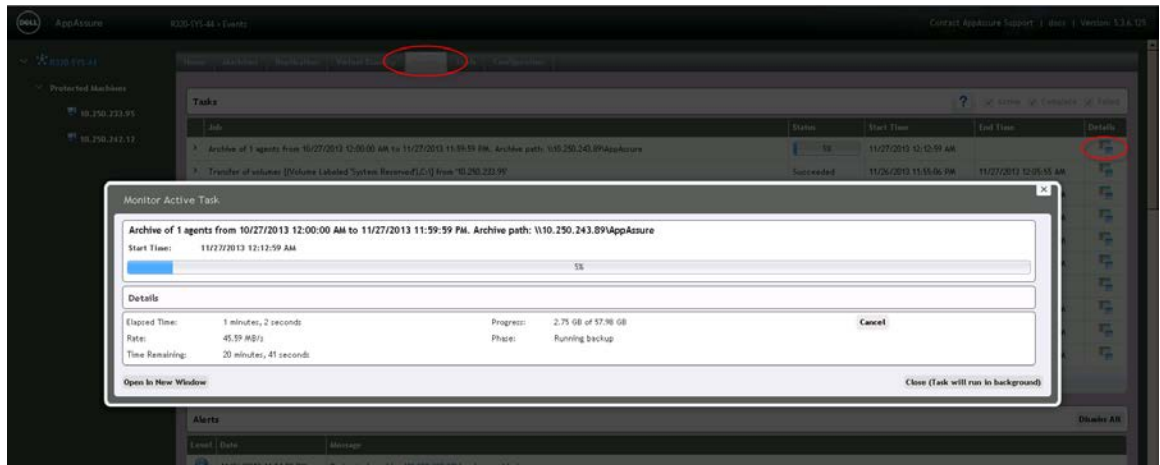

8. AppAssure creates backup images for the protected machines according to the protection policy. To see the backup images, click **Protected Machines** -> **Recovery Points**.
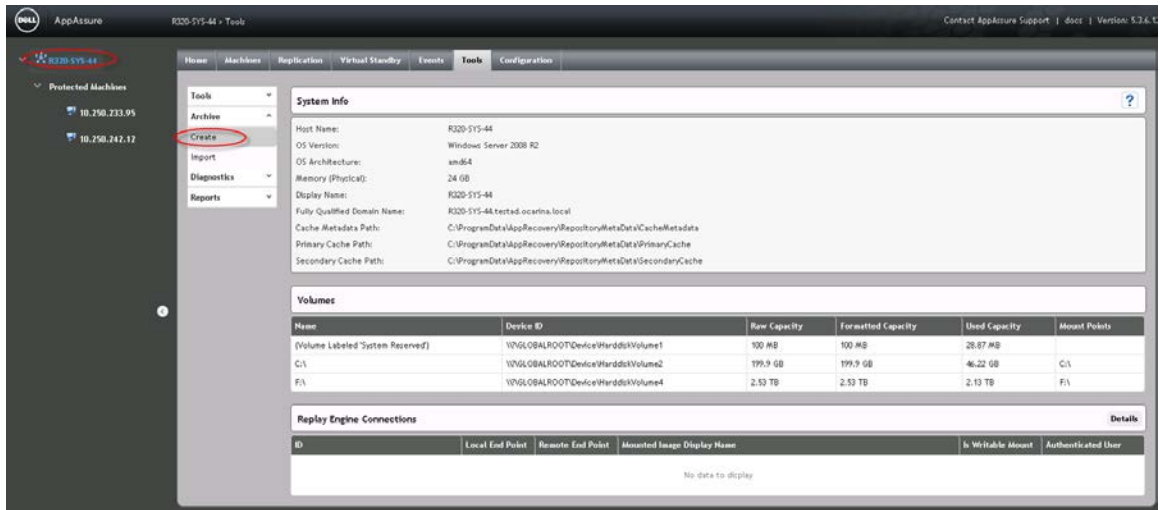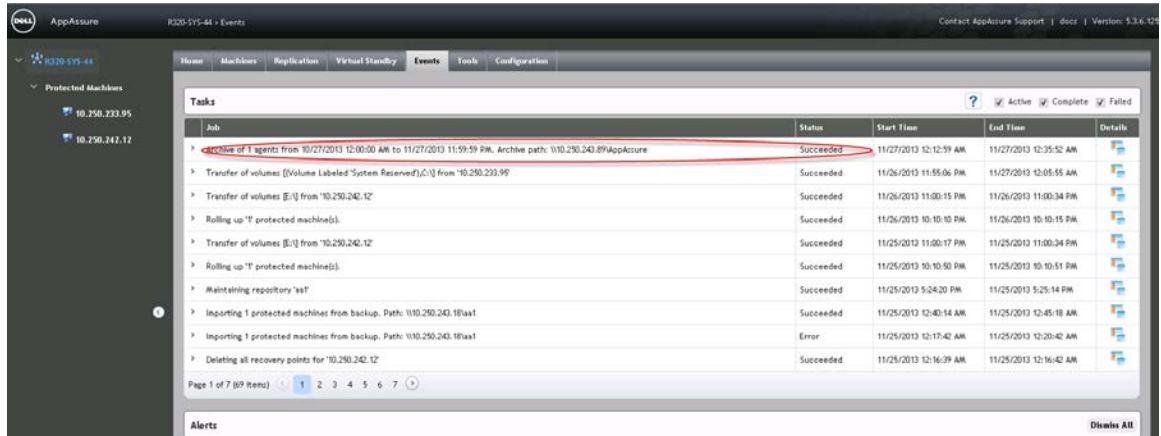
9. To create an archive job, click **Core Server** -> **Tools** -> **Archive** -> **Create**. Enter all of the required information then click **Archive**.
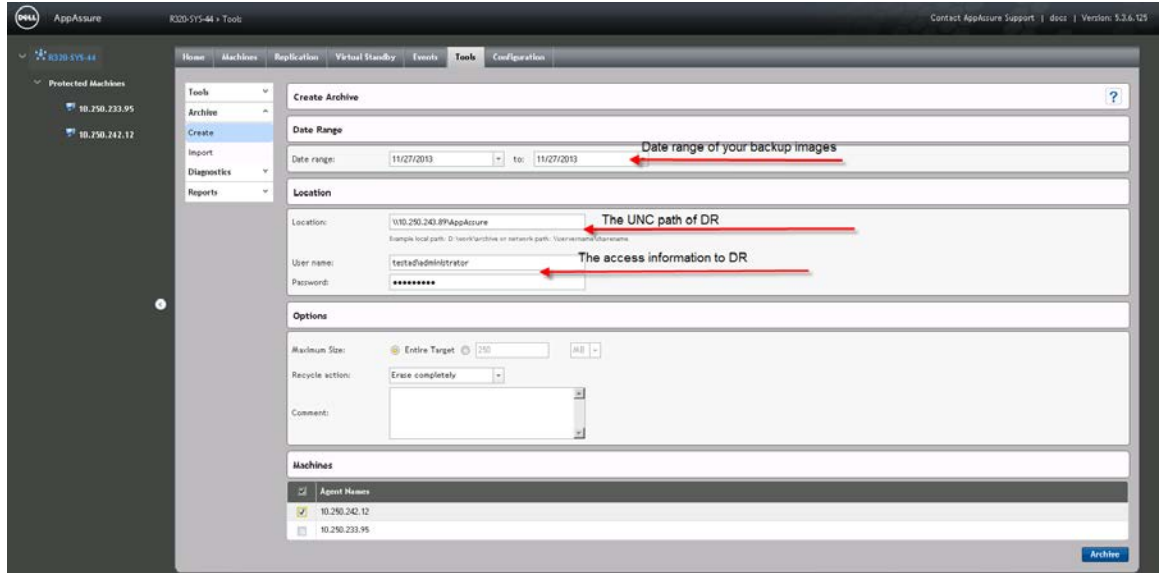
10. To check the archive job details, click the **Events** tab.

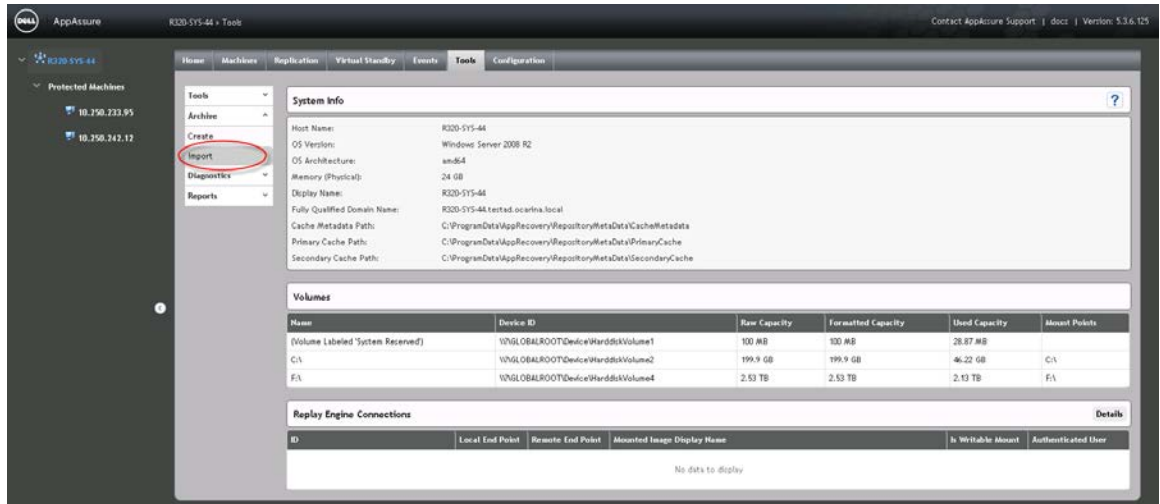11. The archive job details are displayed on the **Events** tab.

12. To return to the **Next Step Wizard** page, click **Finish**. To close the window, click **Close**.
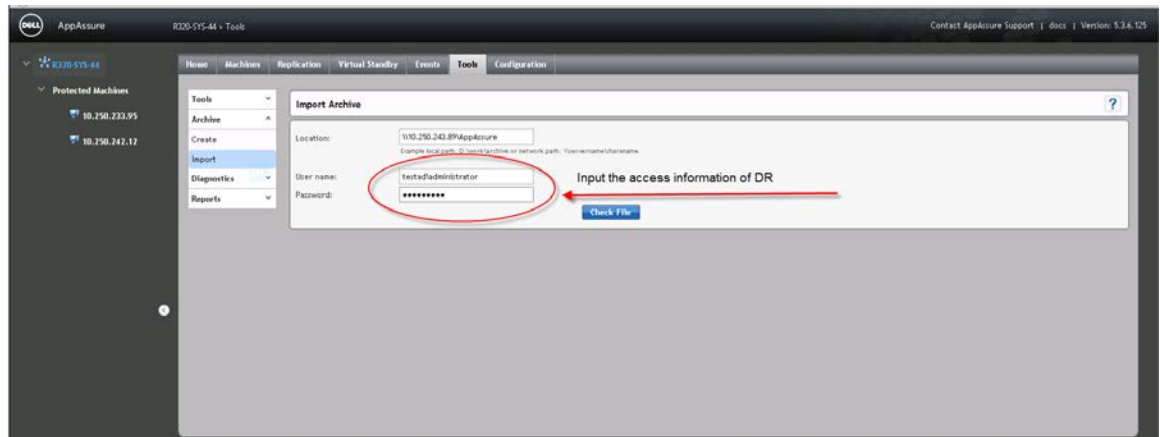
## 2.2 Restoring archived backup images from the DR Series system

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

2. Enter the UNC path of the DR Series system container share that holds the archive images. In addition, enter the CIFS credentials for authenticating to the DR Series system. Click **Check File**.
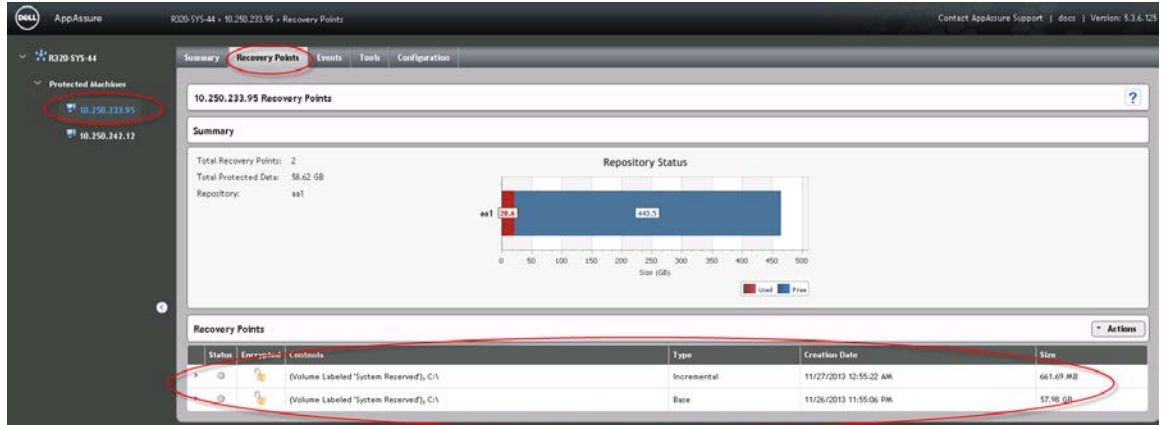
3. Under **Agent Names**, select the agent and repository to which the archived data will be imported and click **Restore**.
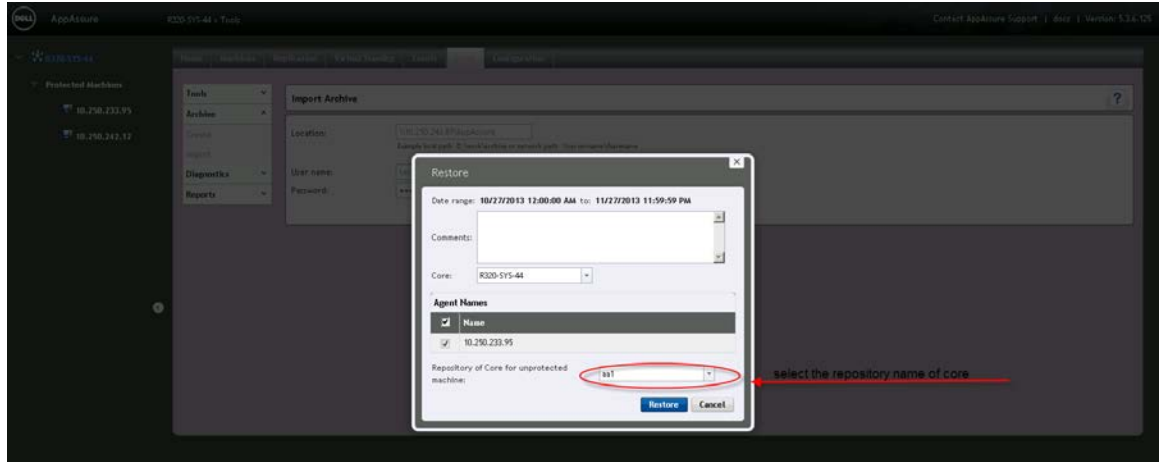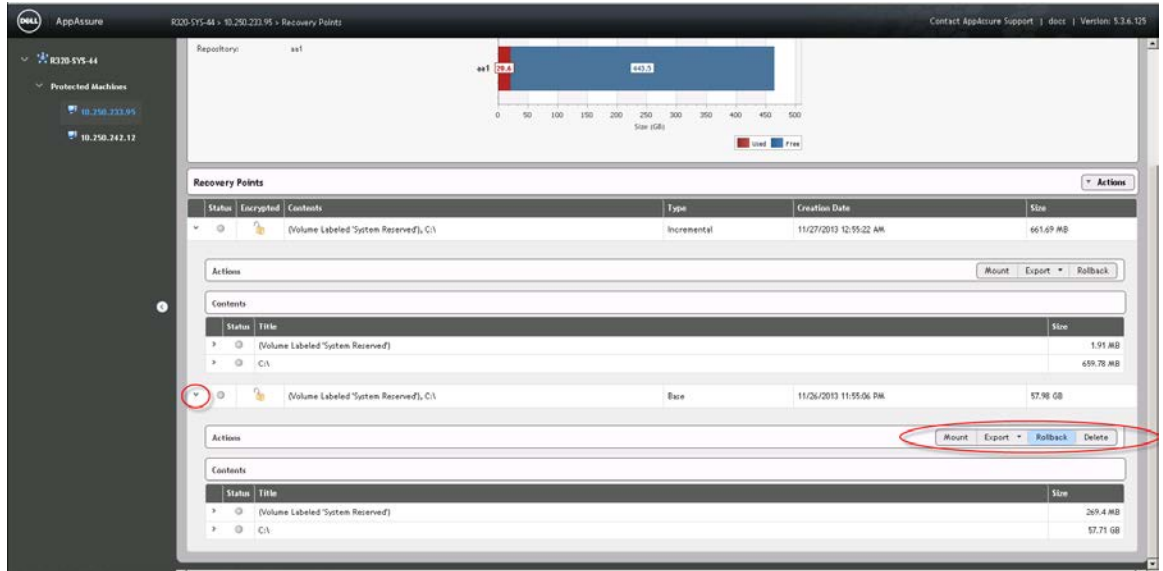

4. To monitor the restore process, click **Open Monitor Window**.
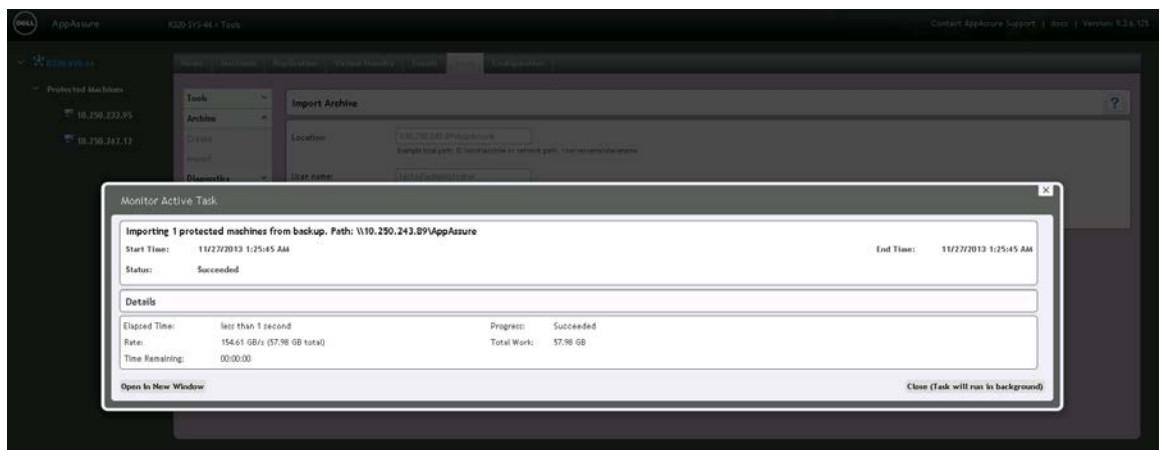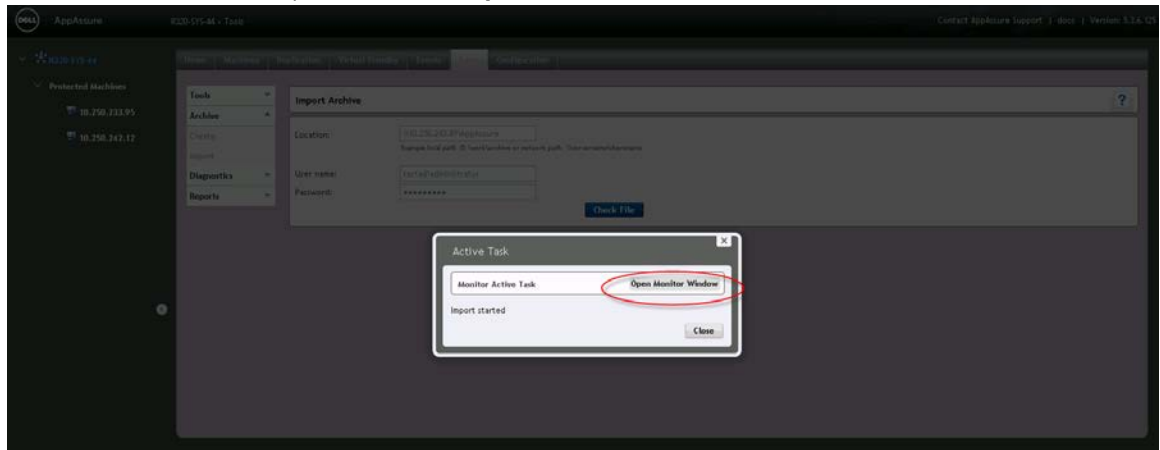
5. After the restore is completed, click **Protected Machines** -> **Recovery Points**. Verify that the recovery point(s) have been restored to the repository.

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

3 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 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 40 hours per week when backups are not taking place, and generally after a backup job has completed.

4 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.
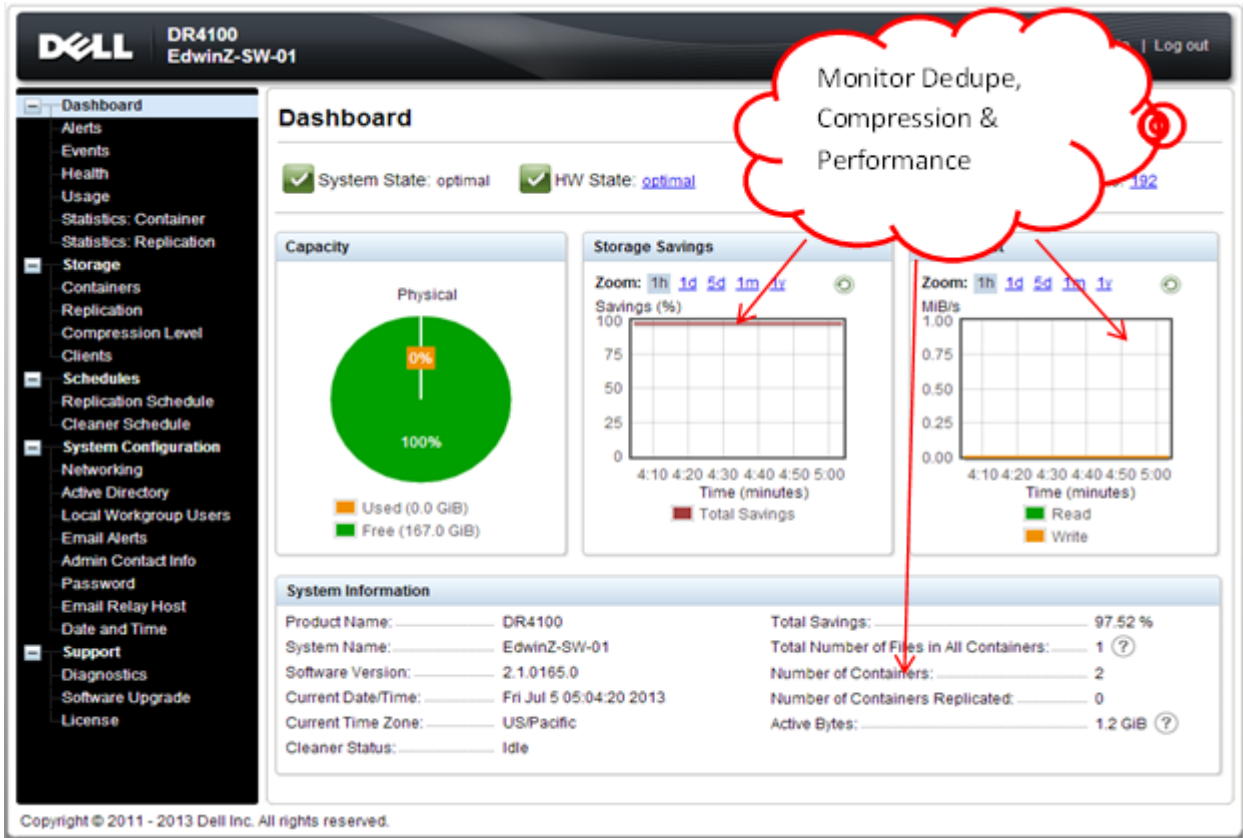
A   Configuring the DR container share as a CIFS storage device on AppAssure

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

- If the DR Series system is joined to an Active Directory domain, you must enter **[domain_name]\user_id** in the **User Name** field for successful authentication.
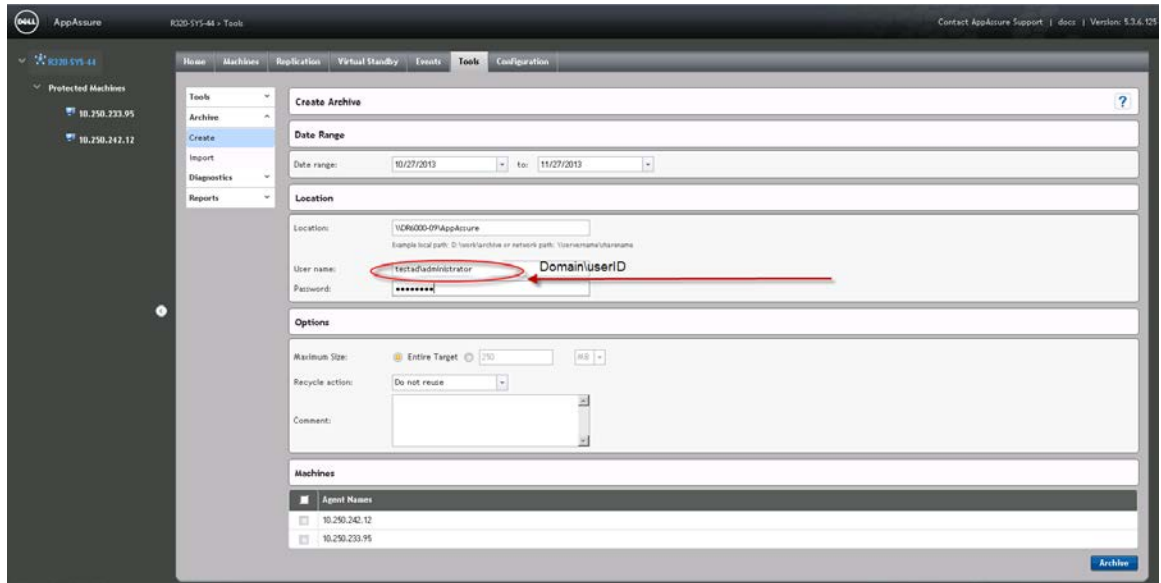
- If the DR Series system is configured as a standalone CIFS server, a DR Series system local CIFS user credential can be used.
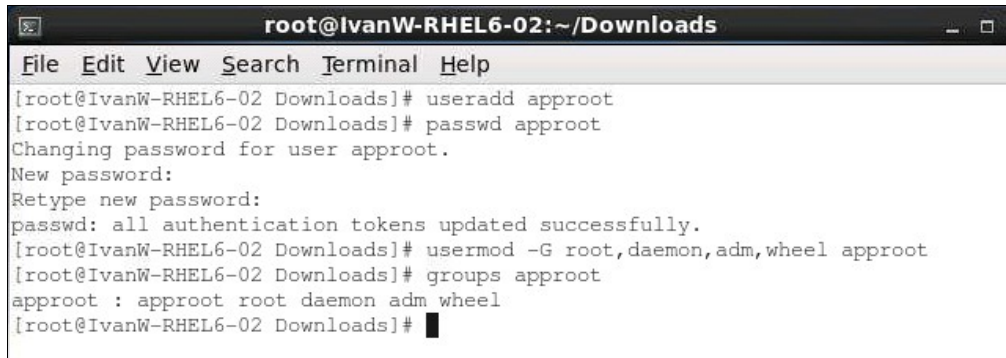
B   Backing up a Linux client

B.1   Installing the Linux agent on 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 the 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_5.4.3.125.sh`

B.2 Backing 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**.
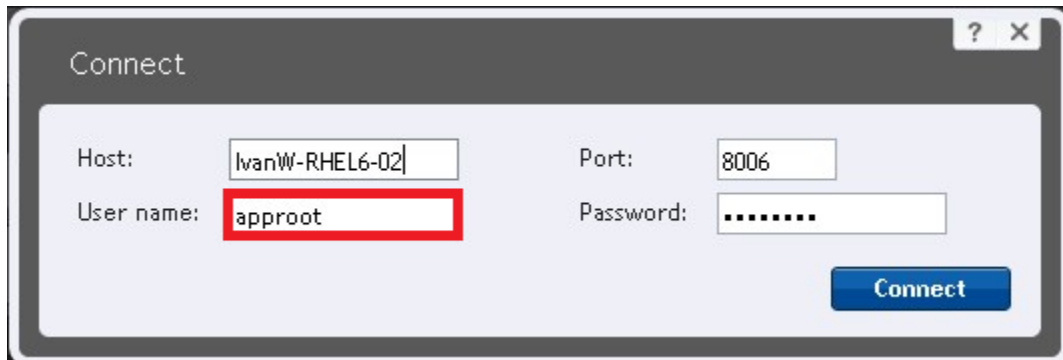
Note: Use the **approot** user, which was added during agent installation.

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