

Setting up the DR Series System with vRanger

Technical White Paper

Quest Engineering

November 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.

Contents

Installing and configuring the DR Series system	5
Configuring a CIFS/NFS container for backup	9
Configuring the NFS share for backup.....	11
Configuring an RDA container for backup.....	13
Creating an RDS container	13
Configuring vRanger	15
Adding a vCenter or ESX host to vRanger	15
Adding a physical client to vRanger	16
Adding a CIFS/NFS repository to vRanger	17
Adding a Quest RDA device to vRanger.....	18
Enabling change block tracking	19
Configuring backup of a machine	20
Configuring RDS repository replication.....	23
Viewing a history of optimized copies	25
Setting up the DR Series system cleaner	26
Monitoring deduplication, compression and performance	28

Executive summary

This document provides information about how to set up the DR Series system with vRanger.

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 vRanger, refer to the vRanger documentation at:

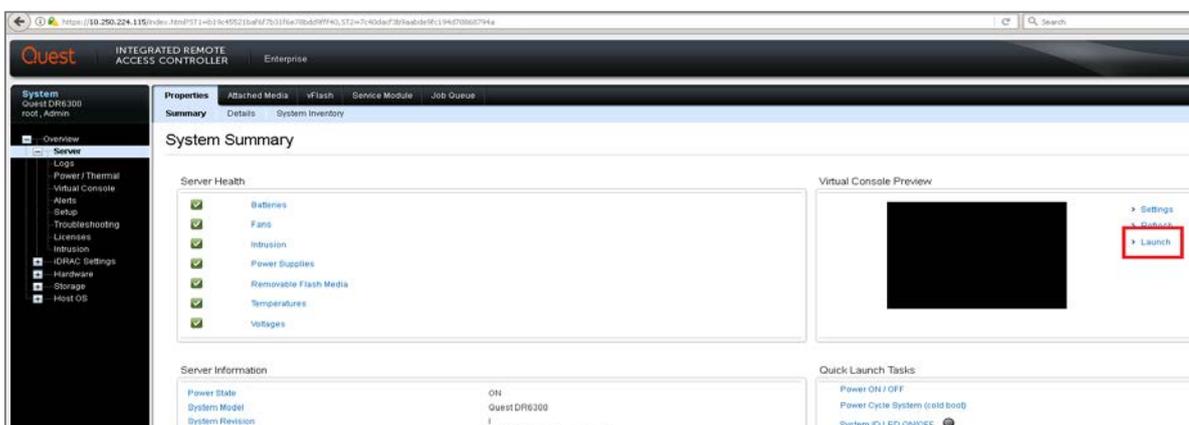
<https://support.quest.com/vranger>



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

Installing and configuring the DR Series system

- 1 Rack and cable the DR Series system, and power it on. In the *Quest DR Series System Administrator Guide*, see the following sections for information about using the iDRAC connection and initializing the appliance.
 - “iDRAC Connection”,
 - “Logging in and Initializing the DR Series system”
 - “Accessing iDRAC6/iDRAC7 Using RACADM”
- 2 Log on to iDRAC using the default credentials (username: **root** and password: **calvin**) and either:
 - the default address **192.168.0.120**,
 - or the IP address that is assigned to the iDRAC interface
- 3 Launch the virtual console.



- 4 When the virtual console opens, log on to the system (with the username: **administrator** and password: **St0r@ge!** where the “0” in the password is the numeral zero).



- 5 Set the user-defined networking preferences.

```
Would you like to use DHCP (yes/no) ?
Please enter an IP address:
Please enter a subnet mask:
Please enter a default gateway address:
Please enter a DNS Suffix (example: abc.com):
Please enter primary DNS server IP address:
Would you like to define a secondary DNS server (yes/no) ?
Please enter secondary DNS server IP address:
```

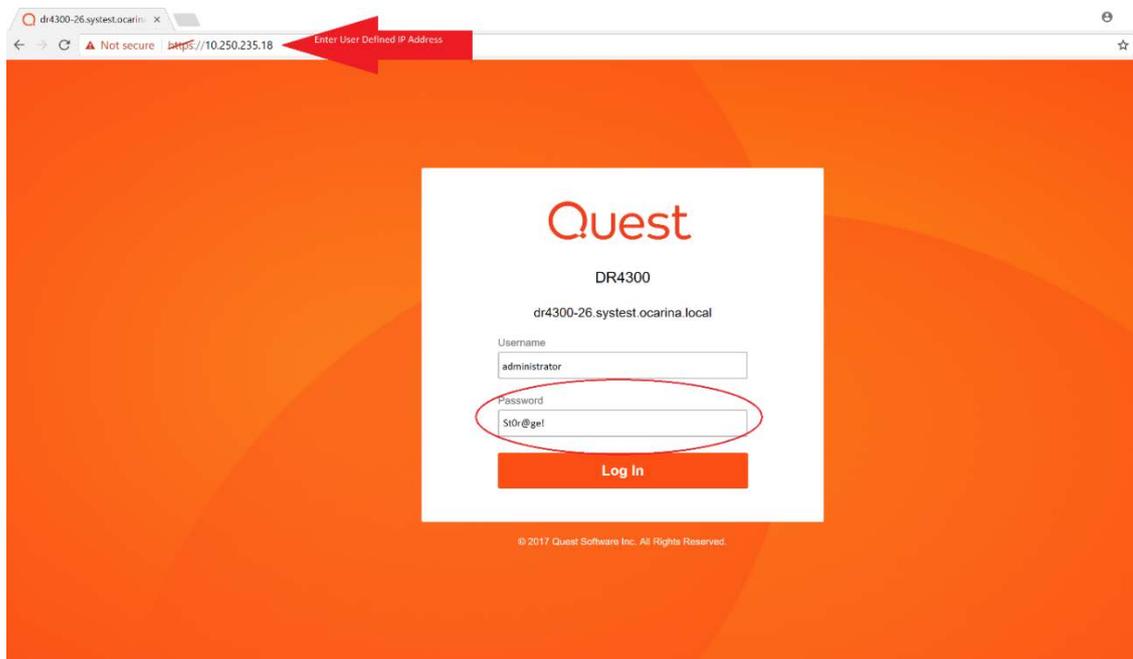
- 6 View the summary of preferences and confirm that it is correct.

```
=====
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) ? _
```

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

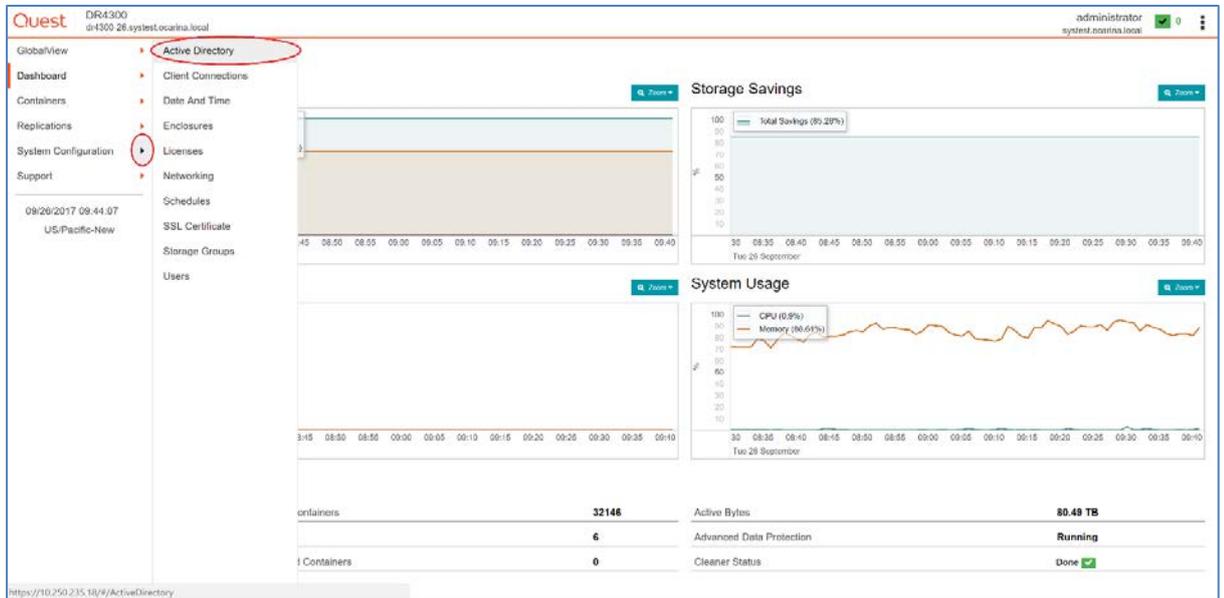


8 Join the DR Series system to Active Directory.

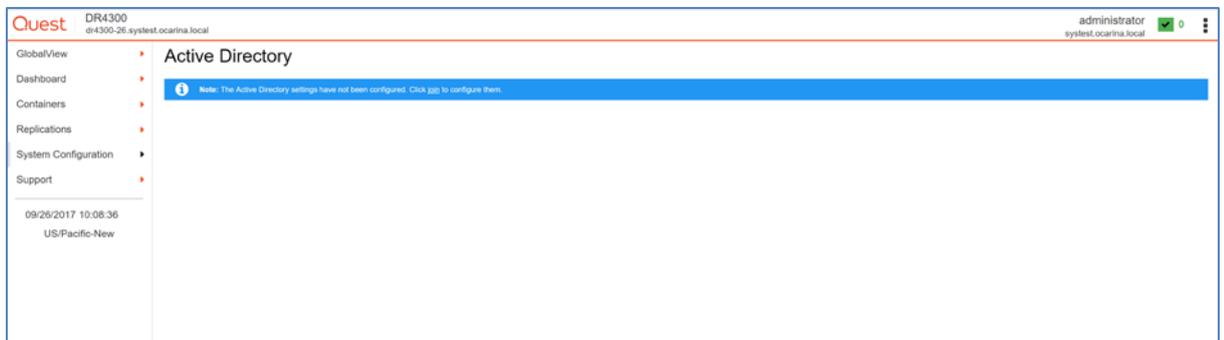


NOTE: if you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

- a In the left navigation area of the DR Series system GUI, click **System Configuration** and then select **Active Directory**.



- b Click **Join**.



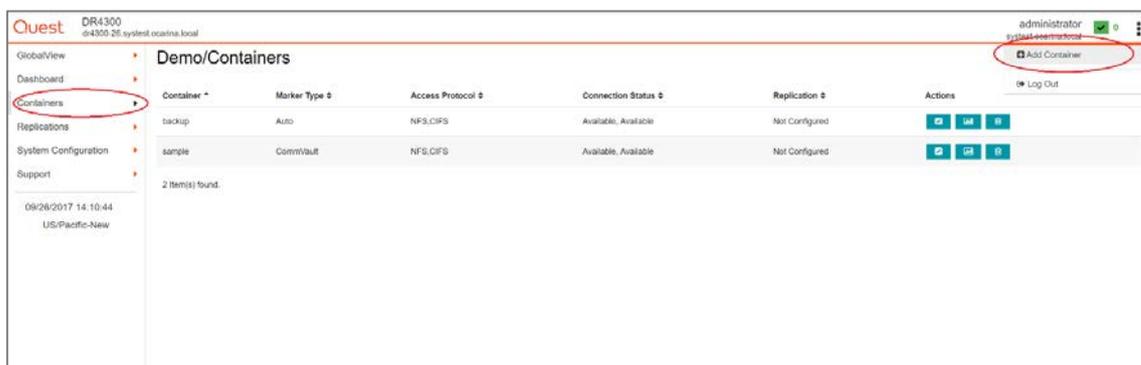
c Enter valid credentials and click **Join**.

The screenshot shows the Quest Active Directory configuration interface. The top bar includes the Quest logo, system information (DR4300, dh4300-25.system.ocarina.local), and user information (administrator, system.ocarina.local). A left sidebar contains navigation options: GlobalView, Dashboard, Containers, Replications, System Configuration, and Support. The main content area is titled 'Active Directory' and features a 'Join' section with the following fields: 'Domain Name (FQDN)' (Required), 'Username' (Required), 'Password' (Required), and 'Org Unit'. At the bottom of the form are 'Join' and 'Cancel' buttons. The bottom left of the interface shows a timestamp '09/26/2017 09:46:45' and the text 'US/Pacific-New'.

Configuring a CIFS/NFS container for backup

Follow these steps to configure CIFS and/or NFS containers for backup.

- 1 In the DR Series system GUI, click **Containers** in the left navigation area, and on the **Action Menu** in the top right of the page, click **Add Container**.



- 2 Enter a Container Name, select **NAS (NFS/CIFS)** for Access Protocol, and click **Next**.



- 3 Select the CIFS or NFS check box as needed, and click **Next**. (vRanger supports both the CIFS and NFS protocols.)

- 4 For NFS, specify the client access credentials and click **Next**.

- 5 For CIFS, specify the client access credentials and click **Next**.

NOTE: For improved security, Quest recommends adding IP addresses for the following (Not all environments will have all components):

- Backup console (vRanger Server)
- ESXi hosts (as vRanger backups up these VMs)
- Backup proxies (for vSphere environments)

- 6 Click **Save** to create the container.

+ Add Container

Storage Access Protocol

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

Container Name **sample**

Configure NAS Access & Marker

NAS Access Protocol **NFS , CIFS**

Marker Type **CommVault**

Configure NFS Client Access

NFS Options **Read Write Access**

Map Root To **Root**

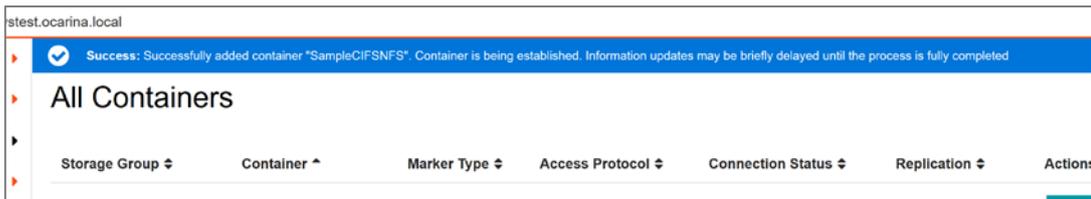
Client Access **Open (allow all clients)**

Configure CIFS Client Access

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

< Previous **Next >** **Save** **✕ Cancel**

- 7 Confirm that the container has been added.



Configuring the NFS share for backup

For NFS backup using vRanger, a target folder must be created in the NFS share directory, which is a sub-directory of the NFS Export directory. This location is where save points are written.

i | **NOTE:** This configuration is not required for adding a CIFS share.

Follow these steps to configure an NFS share for backup in vRanger.

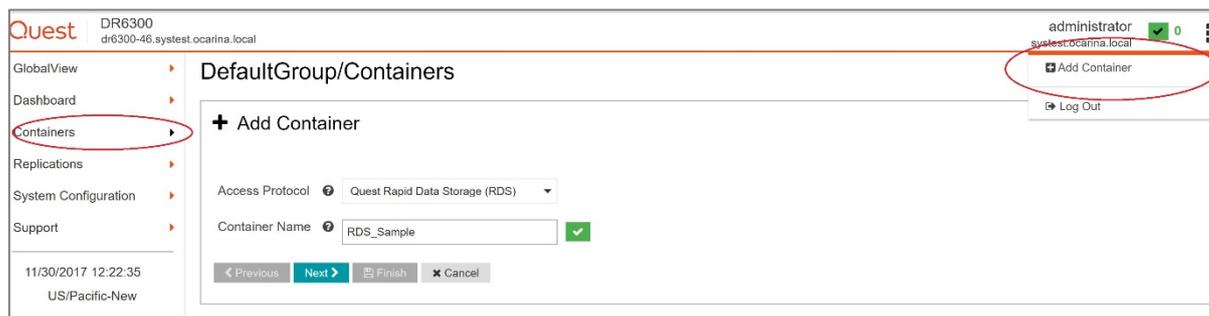
- 1 Mount the NFS share onto any of the NFS clients available in the environment.
- 2 Create a directory using 'mkdir' inside the mounted directory as shown below.

```
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]# mkdir /mnt/mntpt  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]# mount -t nfs 10.250.243.67:/containers/Sample /mnt/mntpt  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]# mkdir /mnt/mntpt/bt  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#  
[root@harika-rh7-v1 ~]#
```

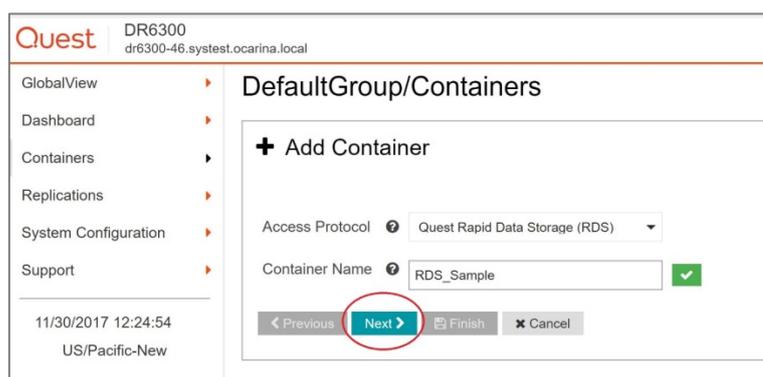
Configuring an RDA container for backup

Creating an RDS container

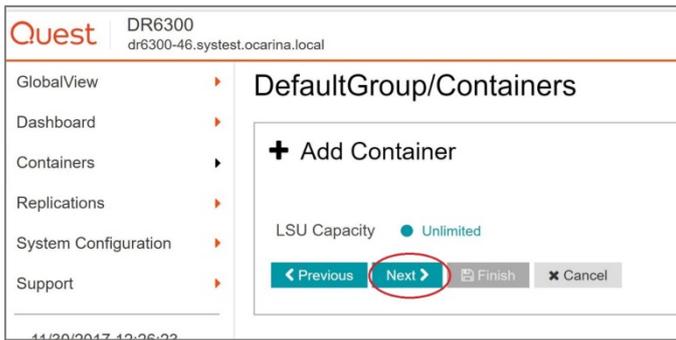
- 1 In the DR Series system GUI, click **Containers** in the left navigation area, and, on the **Action Menu** in the top right of the page, click **Add Container**.



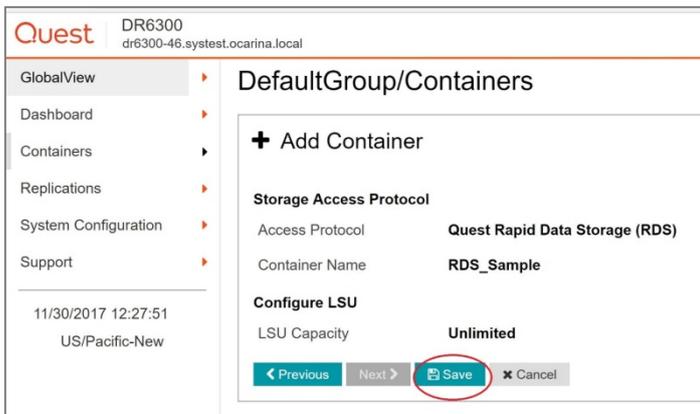
- 2 Select **Quest Rapid Data Storage (RDS)** as the Access Protocol, enter a container name, and click **Next**.



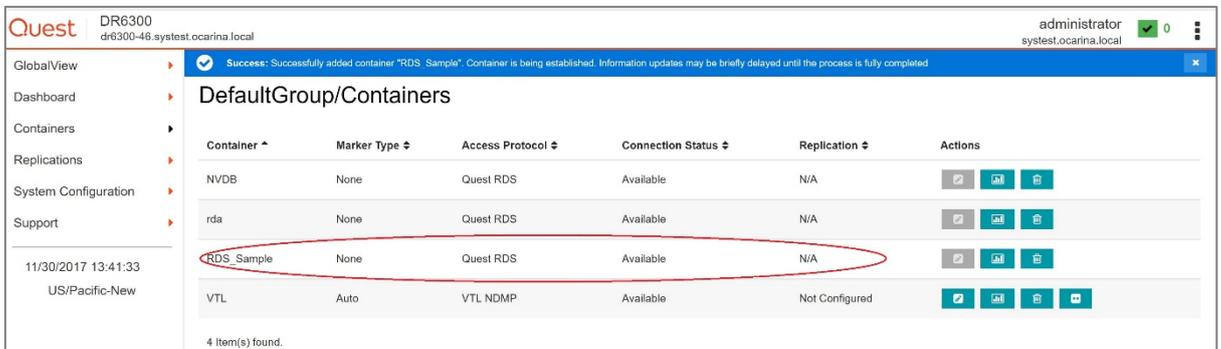
- Verify LSU capacity is set to **Unlimited**, which is the default, and click **Next**.



- Click **Save** to create the RDS container.



- Confirm that the container was added in the list of containers.

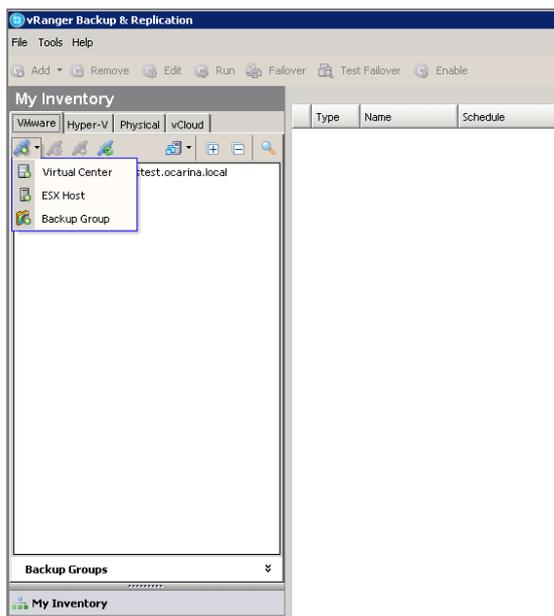


Configuring vRanger

Adding a vCenter or ESX host to vRanger

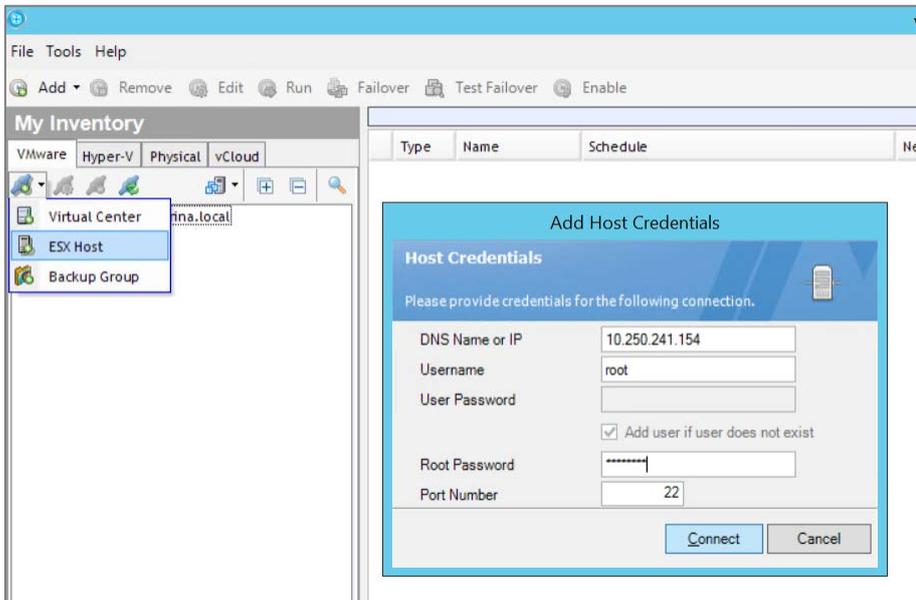
Follow these steps to add a vCenter or ESX host to vRanger.

- 1 In the vRanger Backup and Replication Console, go to **My Inventory**.
- 2 On the VMware tab, click the **Add** icon and add either a vCenter or ESX host.

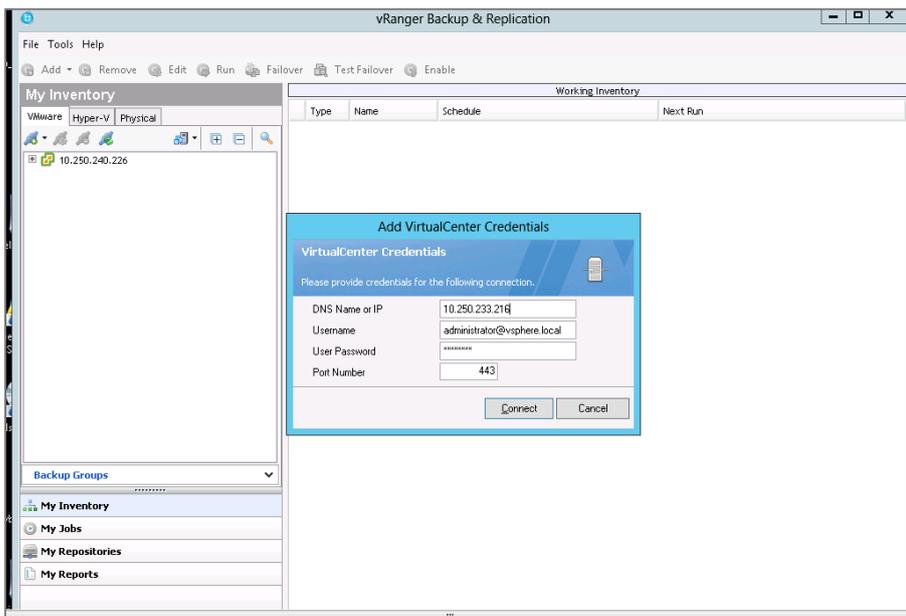


- 3 Provide the IP/Hostname and credentials, and then click **Connect**.

Adding ESX host (Using the root username):



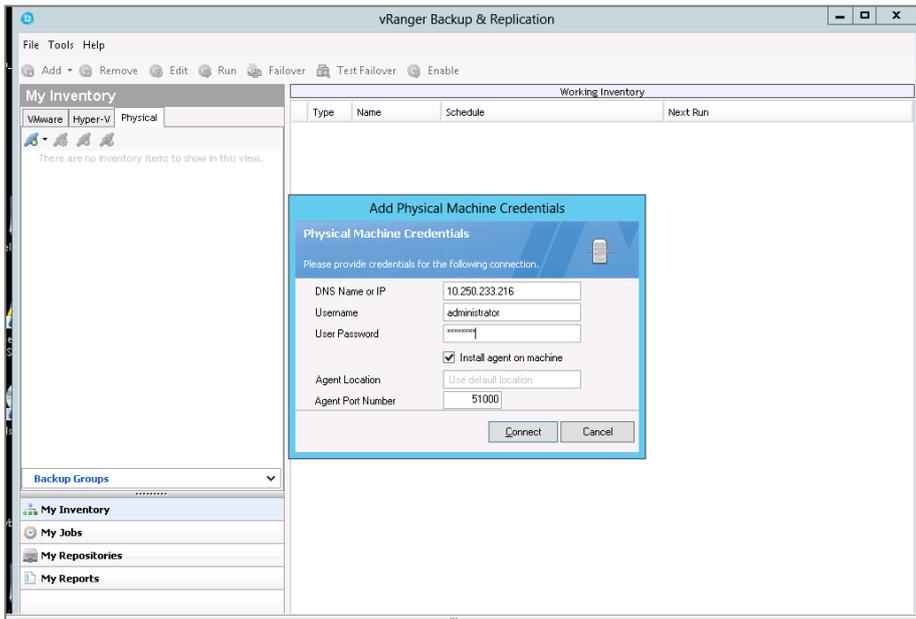
Adding Virtual Center:



Adding a physical client to vRanger

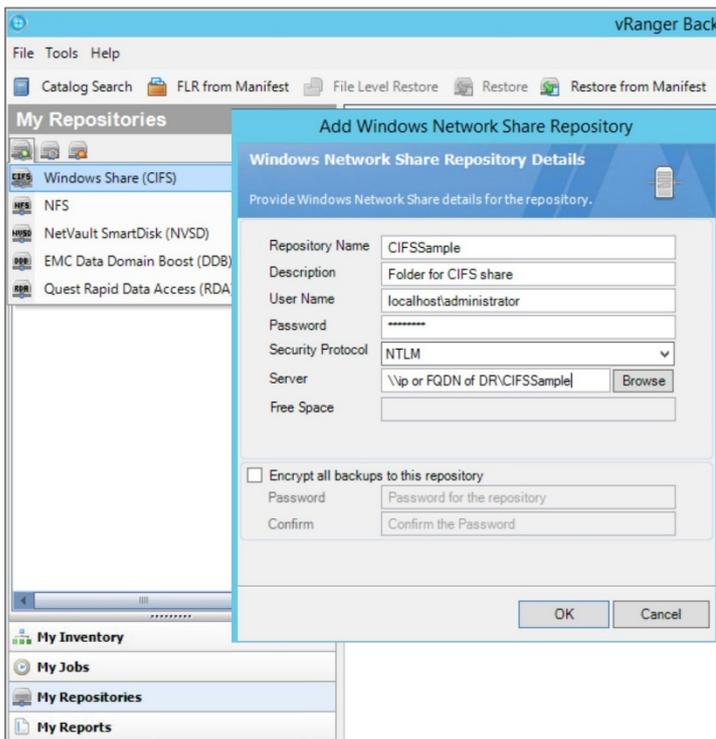
- 1 Navigate to **My Inventory** and, on the **Physical** tab, select the **Add** button and click **Physical Machine**.
- 2 Enter the DNS name or IP address, username, and password.

- 3 Make sure that the **Install agent on machine** checkbox is selected. By default, the physical client is installed on the physical machine at 'c:\programs Files\Quest Software\'.

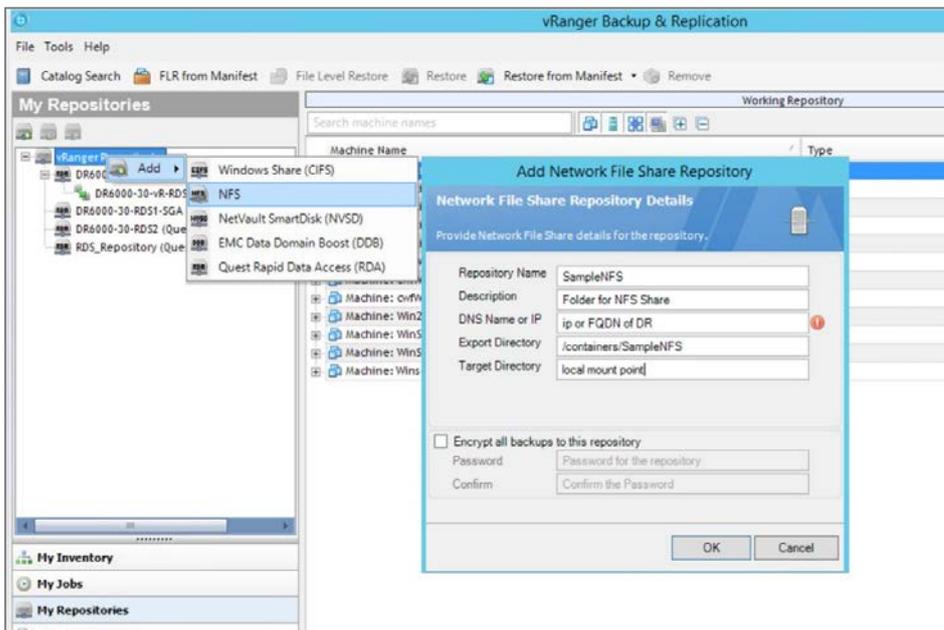


Adding a CIFS/NFS repository to vRanger

- 1 To add a CIFS share, navigate to **My Repositories**, click the **Add** button, select **Windows Share (CIFS)**, enter the required details, and click **OK**. (While creating a repository (CIFS/NFS), for better savings, do not enable encryption.)



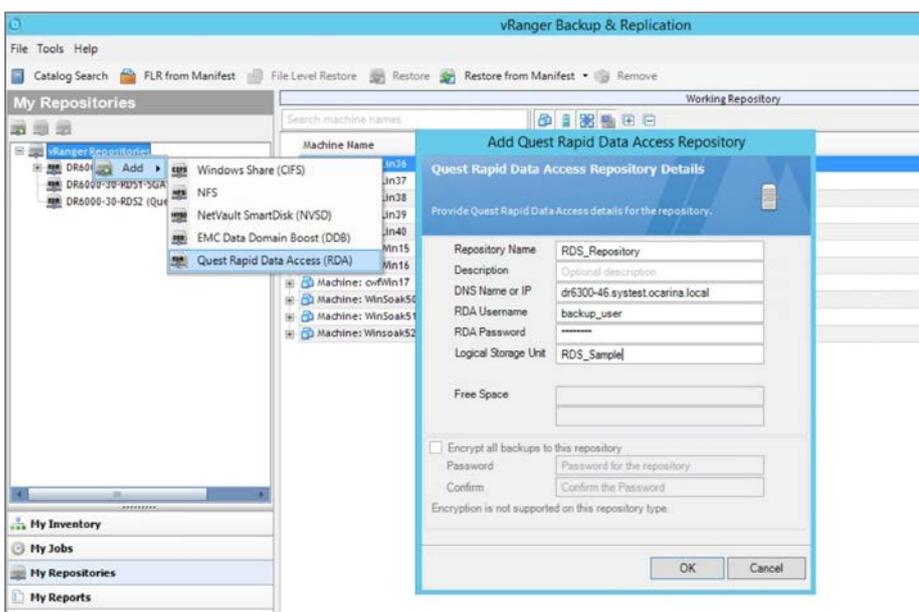
- 2 To add an NFS share, navigate to **My Repositories**, click the **Add** button, select **NFS**, enter the required details, and click **OK**.



NOTE: Export Directory is the folder path to the NFS mount--It should not include the IP/hostname of DR series system. Target Directory refers to the target directory name that was created under the share directory [Mentioned previously in chapter 2].

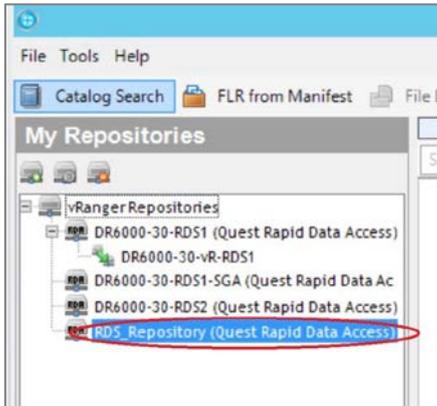
Adding a Quest RDA device to vRanger

- 1 In the vRanger Backup & Replication console, navigate to the My Repositories page, right-click **vRanger Repositories** and click **Add > Quest Rapid Access (RDA)**.



- 2 Enter the hostname or IP address and RDA username and password, enter the container name for the Logical Storage Unit, and click **OK**. (The default username is **backup_user** and the default password is **St0r@ge!** (with the number zero).)

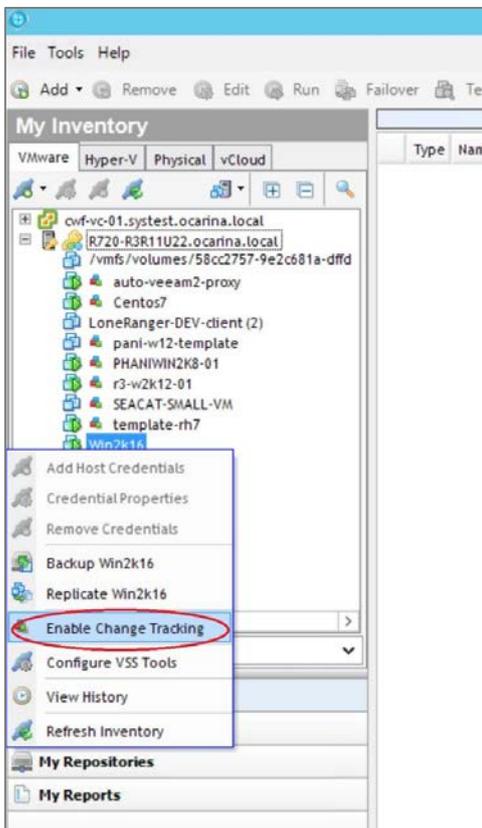
On the **My Repositories** page, you should see the newly added RDA device.



Enabling change block tracking

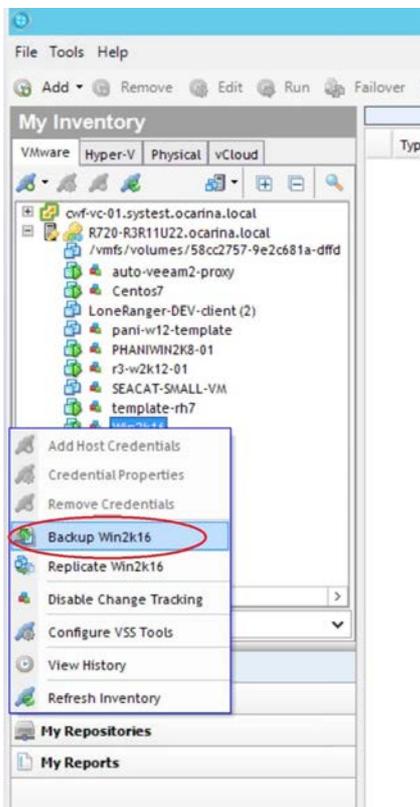
Change block tracking is a VMware technology that allows for tracking of changed blocks on virtual disks. This feature enables quicker, more efficient backups of virtual machines.

- 1 Navigate to **My Inventory**, and on the **VMware** tab, right-click the VM, and select **Enable change tracking**.

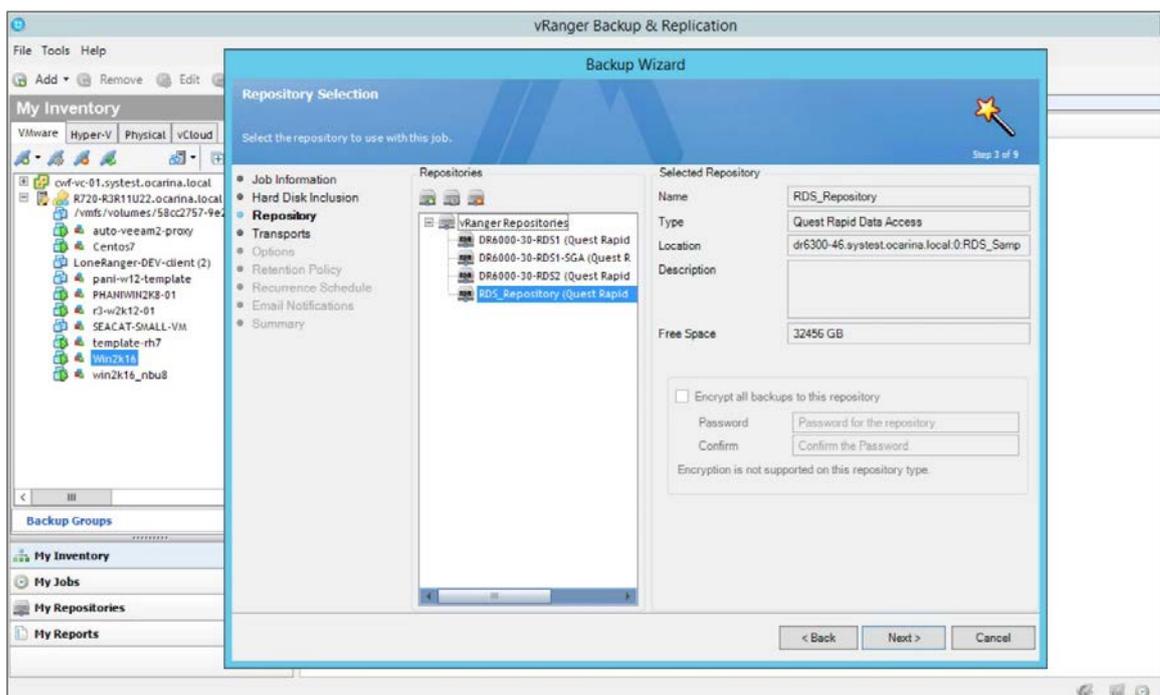


Configuring backup of a machine

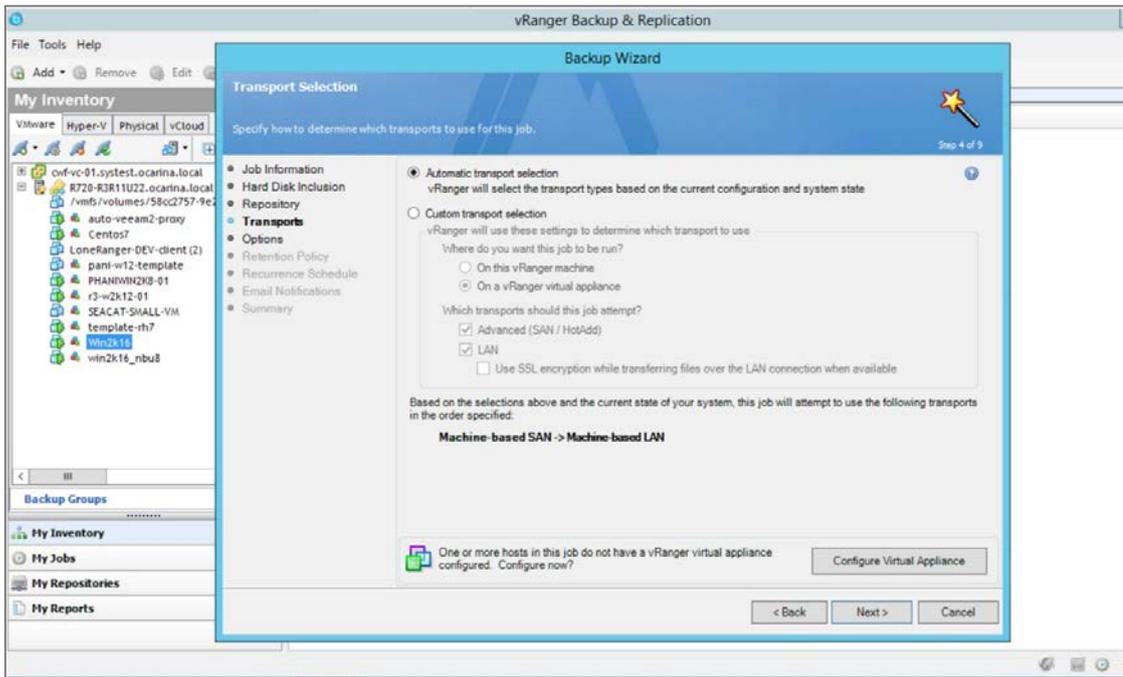
- 1 Navigate to **My Inventory**, right-click the VM or physical machine you want to back up, and click the **Backup** option.



- 2 In the backup wizard, select the disks to backup, select the repository, and click **Next**.

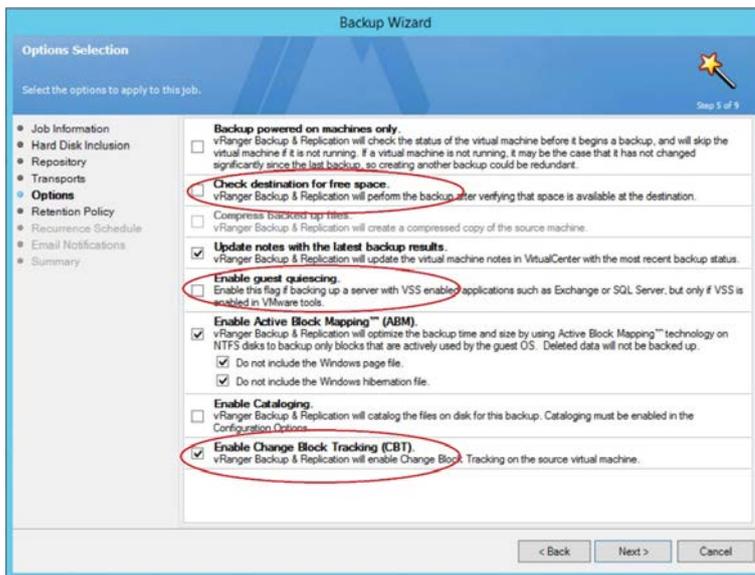


- 3 Select the appropriate Transport type according to your setup, and click **Next**. (If you are unsure, click **Automatic Transport Selection**.)



- 4 In the Backup Options screen, select the following options according to the type of machine.

For VMs:

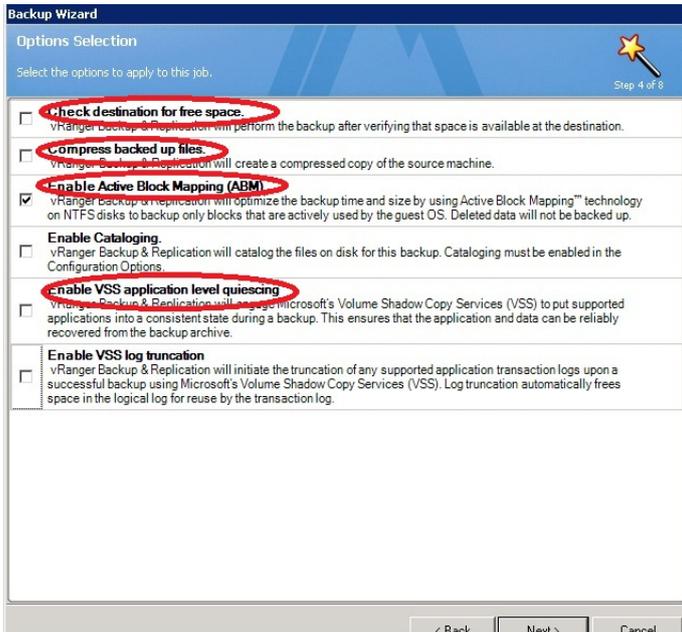


- a Configure the settings as follows:

- Disable '**Check destination for free space**' as the DR series system supports deduplication and so overall space occupied is less.
- Enable **ABM (Active Block Mapping)** for better overall results from both vRanger and the DR Series system.
- Enable '**Guest quiescing**' in case of database backups, for example: Exchange Server.

- Disable '**compress backed up files**' for better savings.

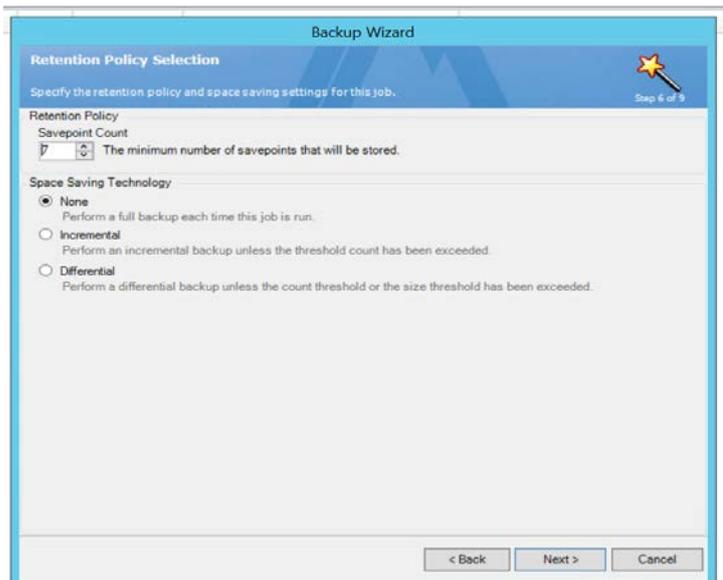
For Physical Machines:



b Configure the settings as follows:

- Disable '**Check destination for free space**' as the DR series system supports deduplication and so overall space occupied is less.
- Enable **ABM (Active Block Mapping)** for better overall results from both vRanger and the DR Series system.
- Enable 'VSS application level quiescing'.
- Disable '**compress backed up files**' for better savings.

5 Apply the required retention policy, and select the backup type.

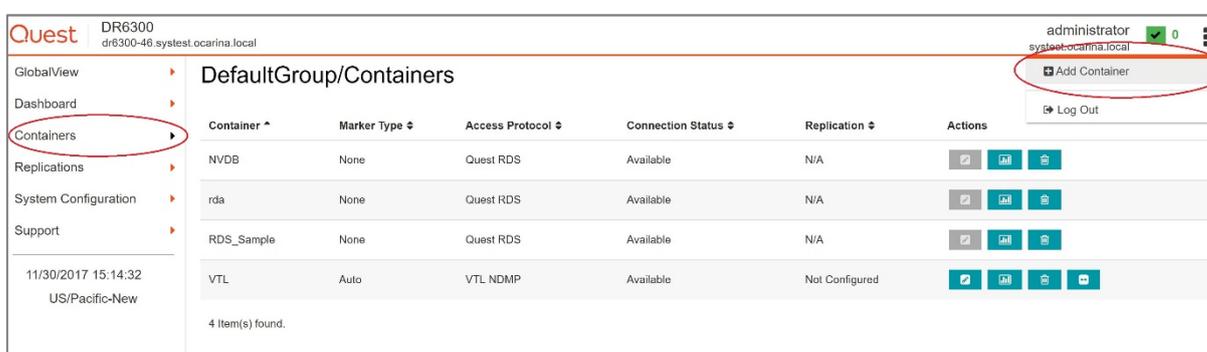


6 Schedule the backup and then enter mail server details for sending mail.

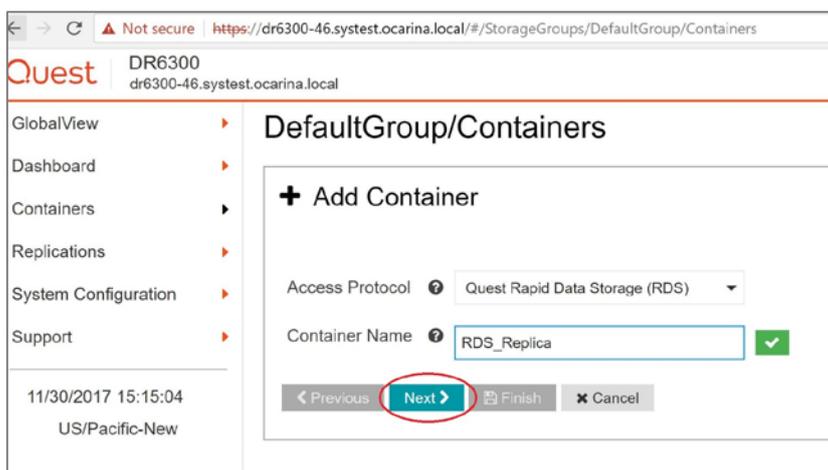
Configuring RDS repository replication

RDA repository replication allows for data to be copied from one DR appliance, optimizing the use of the network between the two devices. Only unique data is sent to the target appliance in this replication. You first need to create a replication target container and then configure vRanger for replication.

- 1 On the replication target DR Series system, click **Containers** in the left navigation area, and, on the **Action Menu** at the top right of the page, click **Add Container**.

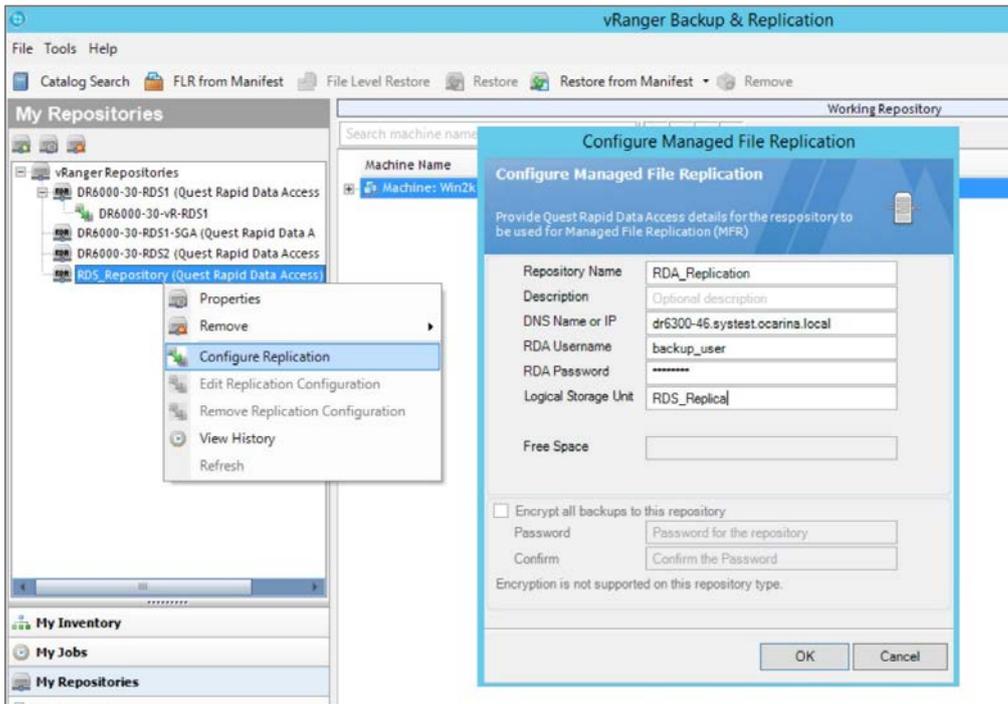


- 2 Select the Protocol type as **Quest Rapid Data Storage (RDS)**, enter a Container Name and click Next.

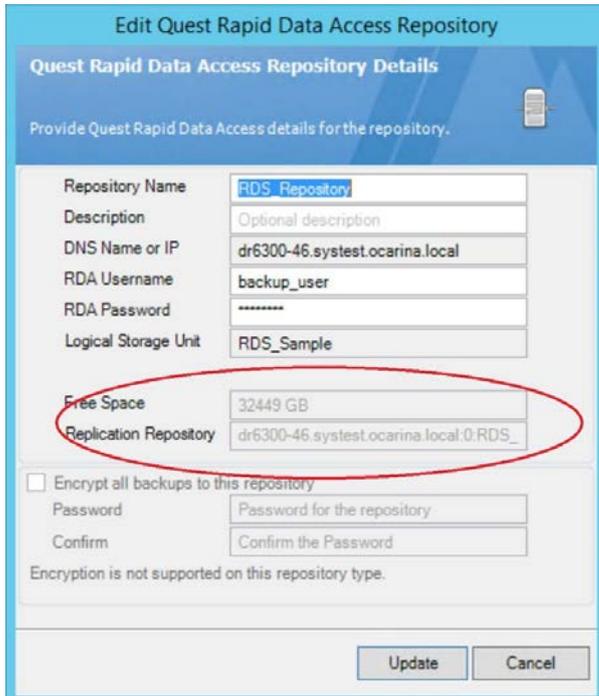


- 3 Complete the container creation steps as described previously in this document.

- In the vRanger console, navigate to **My Repositories**, right-click the source RDA device, click **Configure Replication**, enter the DR appliance and target container details, and click **OK**.



- Confirm replication is configured by right-clicking the RDA repository and clicking **Properties**.



Viewing a history of optimized copies

- 1 In the DR Series system GUI, to view a history of optimized VM copies, click **Containers** in the left navigation area, and, for a selected container, click the **Details** button.

Quest DR6300 dr6300-46.systest.ocarina.local administrator systest.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

All Containers

Storage Group	Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
NVBU-Interop	NVBUONDMP	Auto	VTL NDMP	Available	Not Configured	[Details] [Refresh] [Delete] [More]
NVBU-Interop	NVBUONTAP91	None	VTL (No Access)	Offline	Not Configured	[Details] [Refresh] [Delete] [More]
DefaultGroup	NVDB	None	Quest RDS	Available	N/A	[Details] [Refresh] [Delete] [More]
DefaultGroup	rda	None	Quest RDS	Available	N/A	[Details] [Refresh] [Delete] [More]
DefaultGroup	RDS_Replica	None	Quest RDS	Available	N/A	[Details] [Refresh] [Delete] [More]
DefaultGroup	RDS_Sample	None	Quest RDS	Available	N/A	[Details] [Refresh] [Delete] [More]
DefaultGroup	VTL	Auto	VTL NDMP	Available	Not Configured	[Details] [Refresh] [Delete] [More]

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

- 2 Expand **Duplication** to check the Duplication statistics.

Quest DR6300 dr6300-46.systest.ocarina.local administrator systest.ocarina.local

GlobalView
Dashboard
Containers
Duplication
Replications
System Configuration
Support

Capacity Unlimited Total Images 16

Duplication

Inbound		Outbound	
Bytes Copied (logical)	51 GiB	Bytes Copied (logical)	0 bytes
Bytes Transferred (actual)	13MiB	Bytes Transferred (actual)	0 bytes
Network Bandwidth Savings	99.97 %	Network Bandwidth Savings	0.00 %
Current Count Of Active Files	15	Current Count Of Active Files	0
Replication Errors	0	Replication Errors	0

Active Optimized Copies

File Name

No records

History of Optimized Copies

File Name

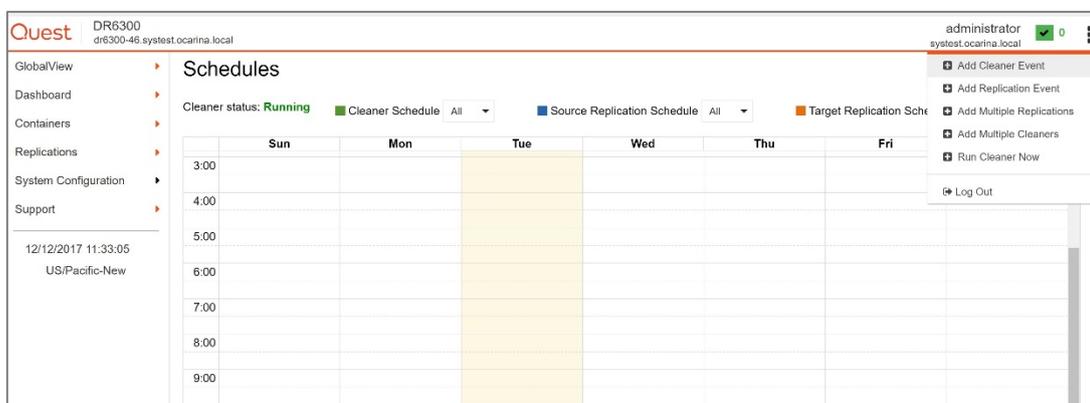
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171130_145805_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171130_145805_F.Manifest.metadata
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171130_150148_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171130_150148_F_1_Win2k16_vmdk.var
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171130_150148_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171130_150148_F.VmConfig.metadata
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171130_150148_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171130_150148_F.Manifest.metadata
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171212_103159_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171212_103159_F_1_Win2k16_vmdk.var
- /Win2k16_4201d728-4ad6-6df6-0c76-1be8b0cec472/Win2k16_20171212_103159_fa461740-7747-4e90-9563-e6ce7c18798b/Win2k16_20171212_103159_F.VmConfig.metadata

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 system 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 example 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. Refer to the *DR Series Cleaner Best Practices* white paper for guidance on setting up the cleaner.

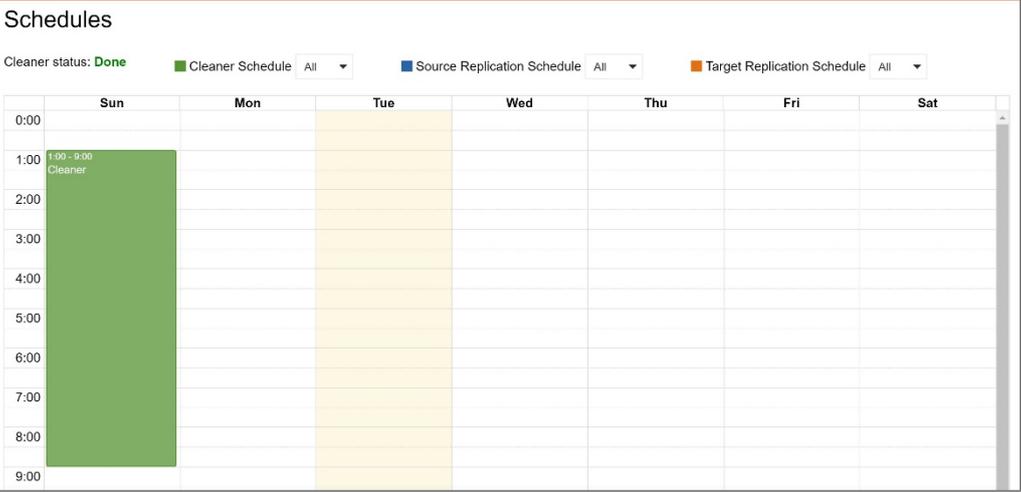
- 1 In the DR Series system GUI, click **System Configuration > Schedules**.
- 2 On the Action menu, click **Add Cleaner Event**.



- 3 Define the schedule and click **Save**.

The screenshot shows the 'New' dialog box for creating a cleaner event. The dialog has a title 'New' and a warning icon with the text 'Only one cleaner event is allowed per day.' Below the warning, there are fields for 'Set event from start day: Sunday at 01:00 to end day: Sunday at 09:00'. The 'Save' button is highlighted in blue, and the 'Cancel' button is in grey.

The new cleaner event is displayed on the Schedules page.



Monitoring deduplication, compression and performance

After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput in 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.

