Quest™

Setting up the DR Series System on Acronis Backup & Recovery v11.5

Technical White Paper

Quest Engineering

November 2017

Patents

Trademarks

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

Setting up the DR Series System on Acronis Backup & Recovery v11.5

Updated – December 22, 2017

Contents

Revisions

Date	Description
April 2015	Initial release
October 2016	Updated the guide with new DR 4.0 GUI screens
November 2017	Updated with new Quest-branded DR Series system screenshots (v4.0.3)

Executive Summary

This document provides information about how to set up the DR Series system as a backup target for Acronis v11.5.

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 Acronis, refer to the Acronis documentation at:

https://www.acronis.com/en-us/support/documentation/ABR11.5/index.html#14080.html

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

Installing and configuring the DR Series system

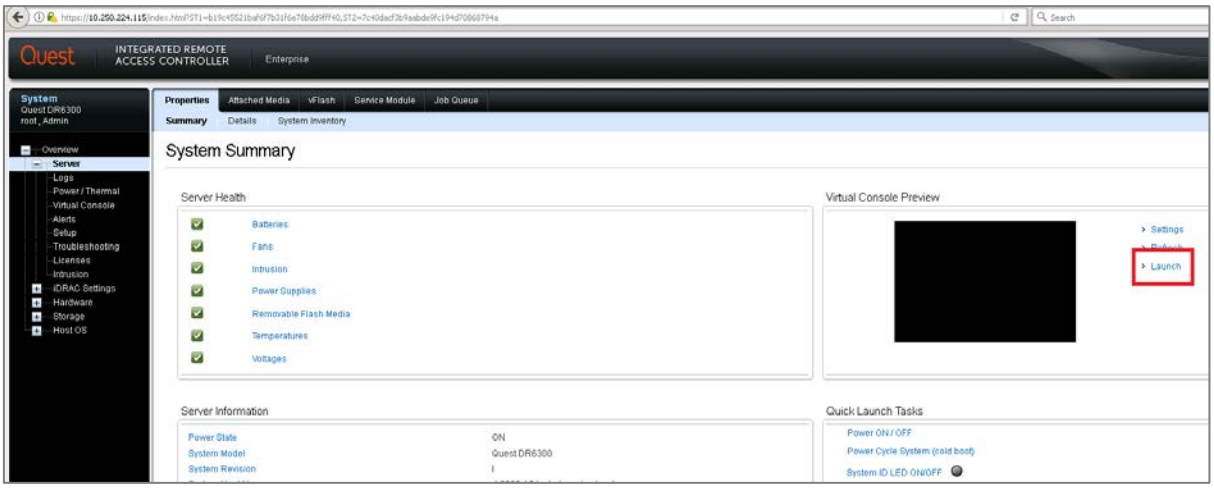
1 Rack and cable the DR Series system, and power it on. In the *DR Series System Administrator Guide*, see the following sections for information about using the iDRAC connection and initializing the appliance.

- "iDRAC Connection",
- "Logging in and Initializing the DR Series system"
- "Accessing IDRAC6/Idrac7 Using RACADM"

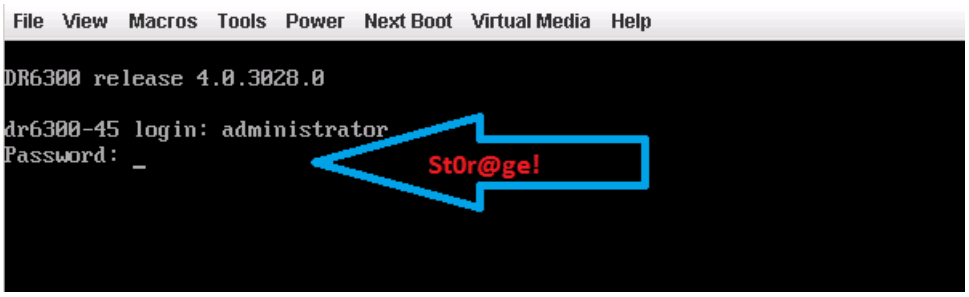
2 Log on to iDRAC using the default credentials (username: **root** and password: **calvin**) and either:

- the default address **192.168.0.120**,
- or the IP address that is assigned to the iDRAC interface

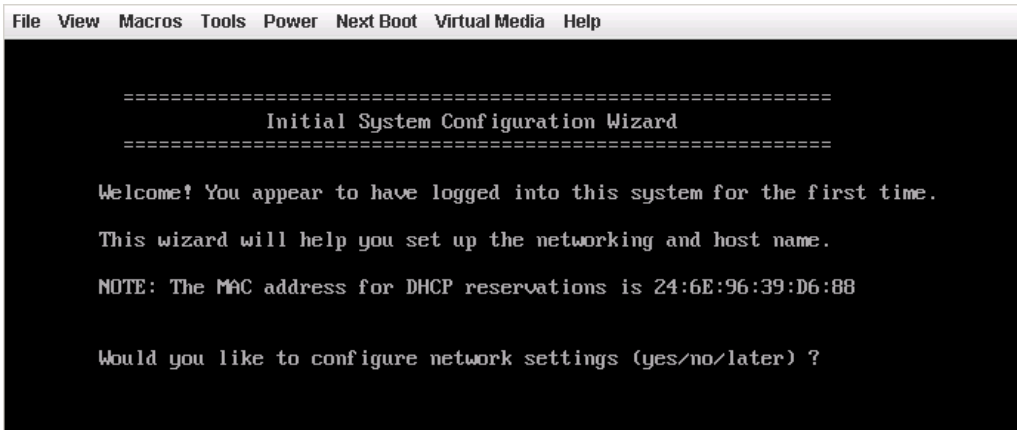
3 Launch the virtual console.



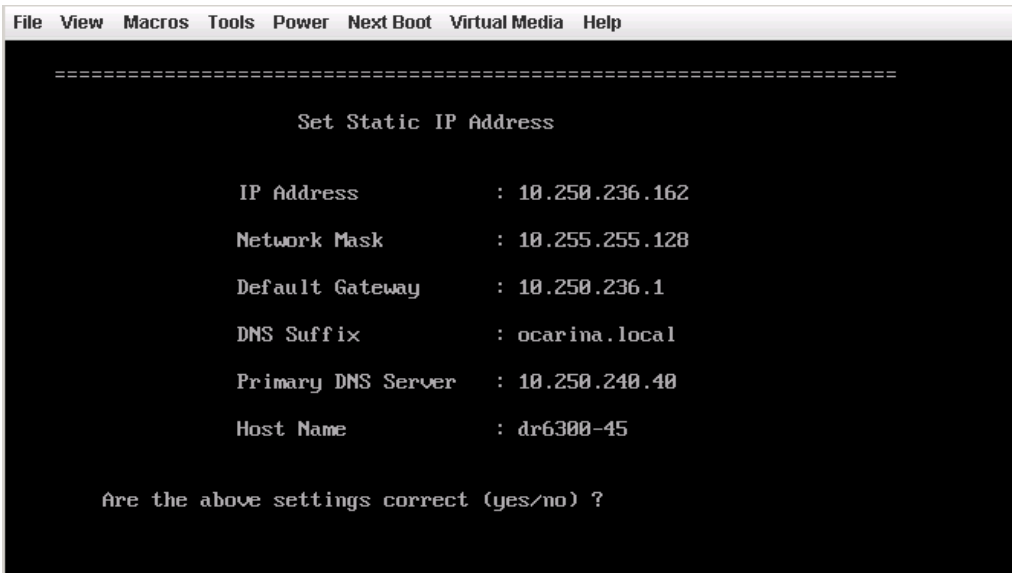
4 After the virtual console opens, log on to the system (with the username: **administrator** and password: **St0r@ge!** where the "0" in the password is the numeral zero).



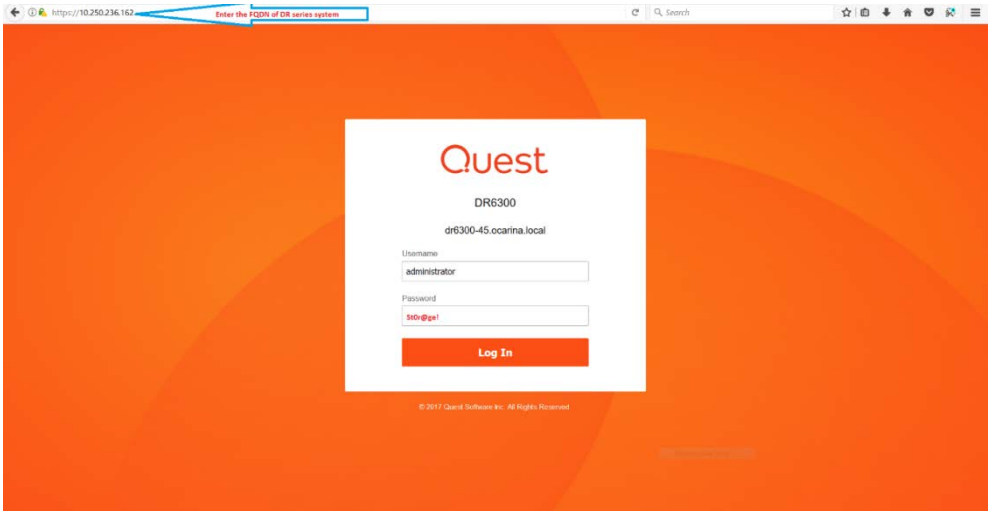
5 Set the user-defined networking preferences.



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



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

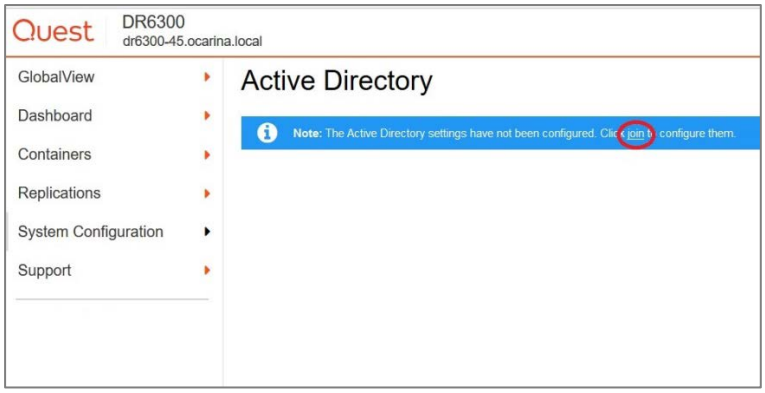


8 Join the DR Series system to Active Directory.

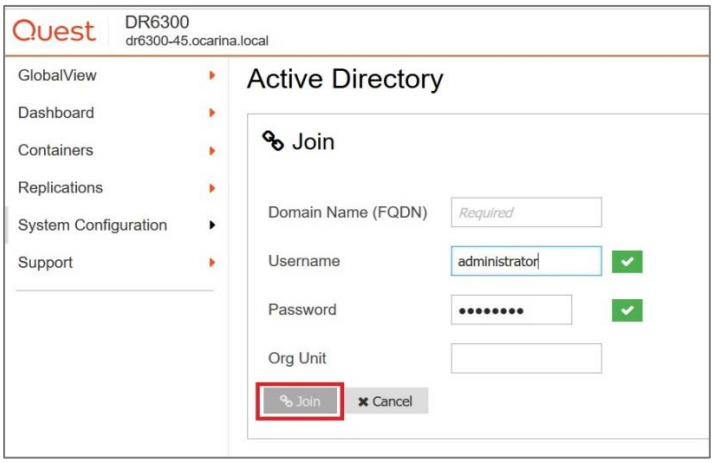
NOTE: If you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

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

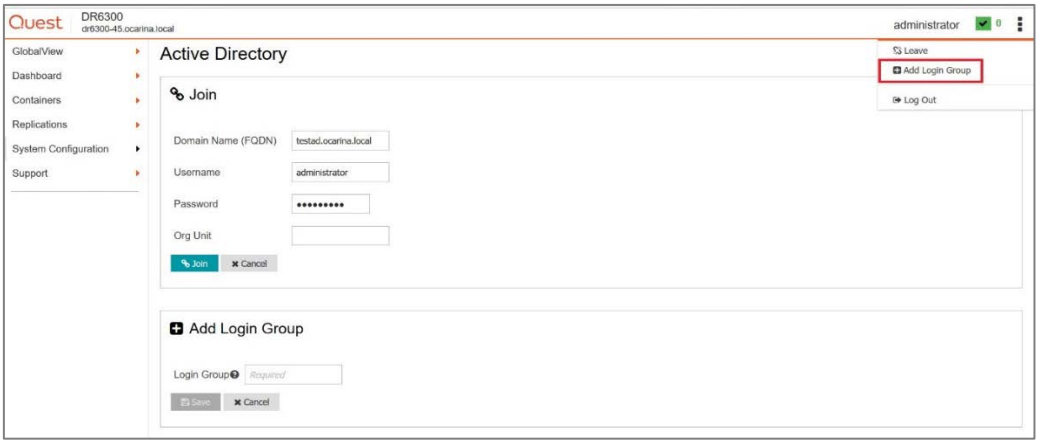
b Click **Join**.



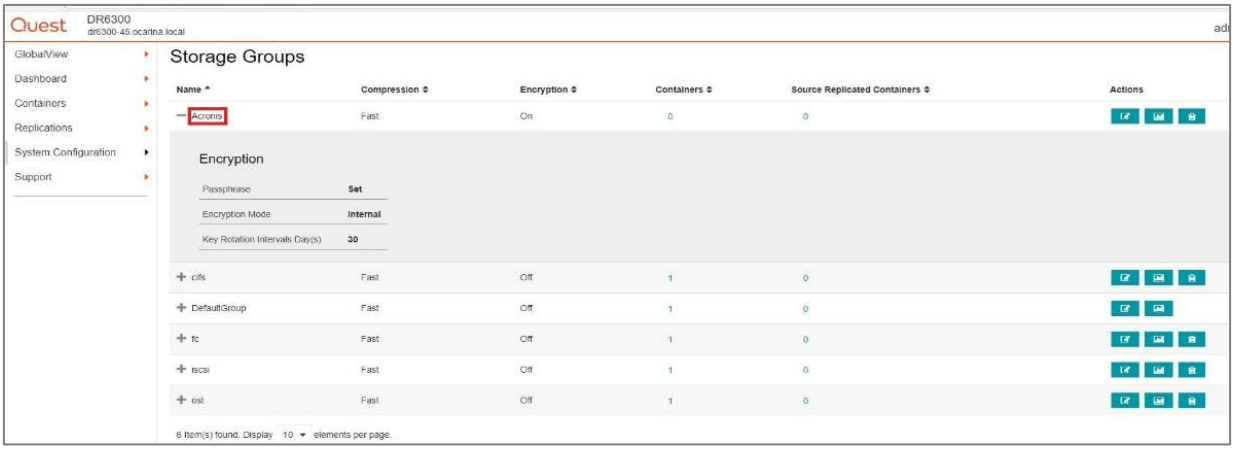
c Enter valid credentials and click **Join**.



d On the Action menu in the upper right corner of the page, click **Add Login Group**.



9 Now you need to create and mount the container. In the left navigation menu, click **Containers.**

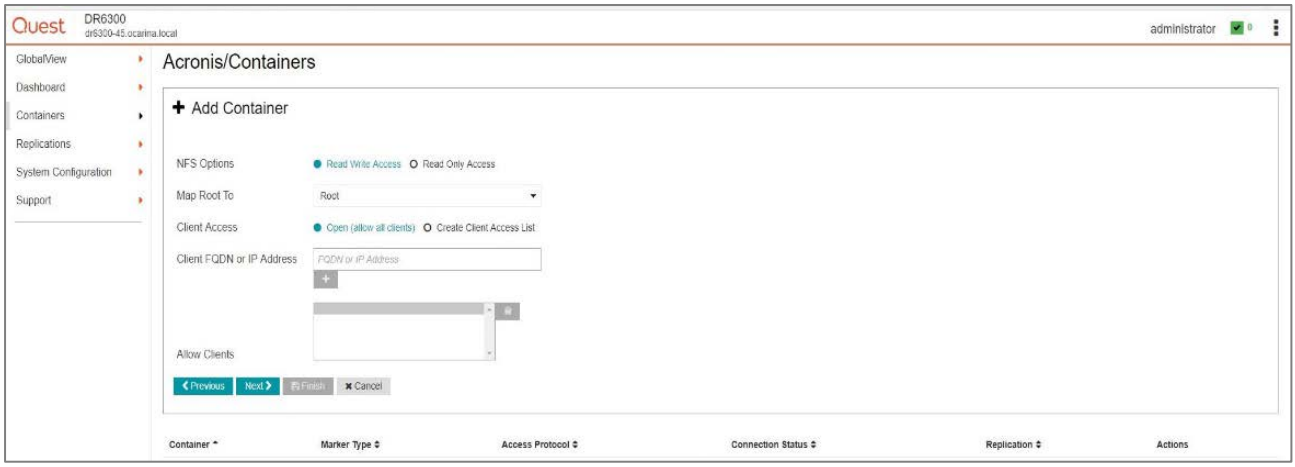


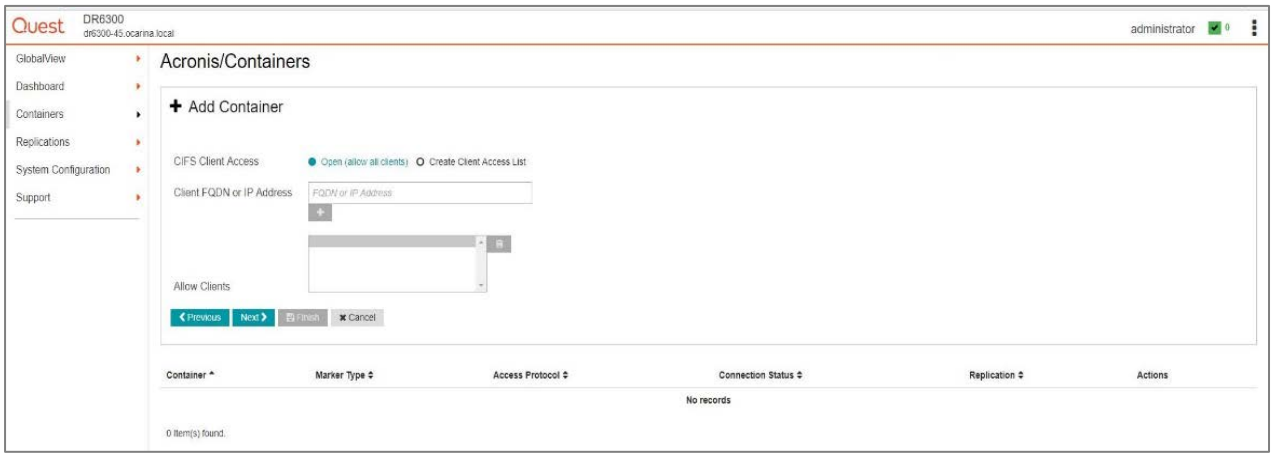
10 On the Action menu in the upper right corner of the page, click **Add Container**.

11 Enter a container name and for the Access Protocol, select **NAS (NFS, CIFS)** and then click **Next**.

12 Select **NFS, CIFS** as the access protocol and the Marker Type as **Auto**, and then click **Next**.

13 Configure the NFS and CIFS client access settings and click **Next**.





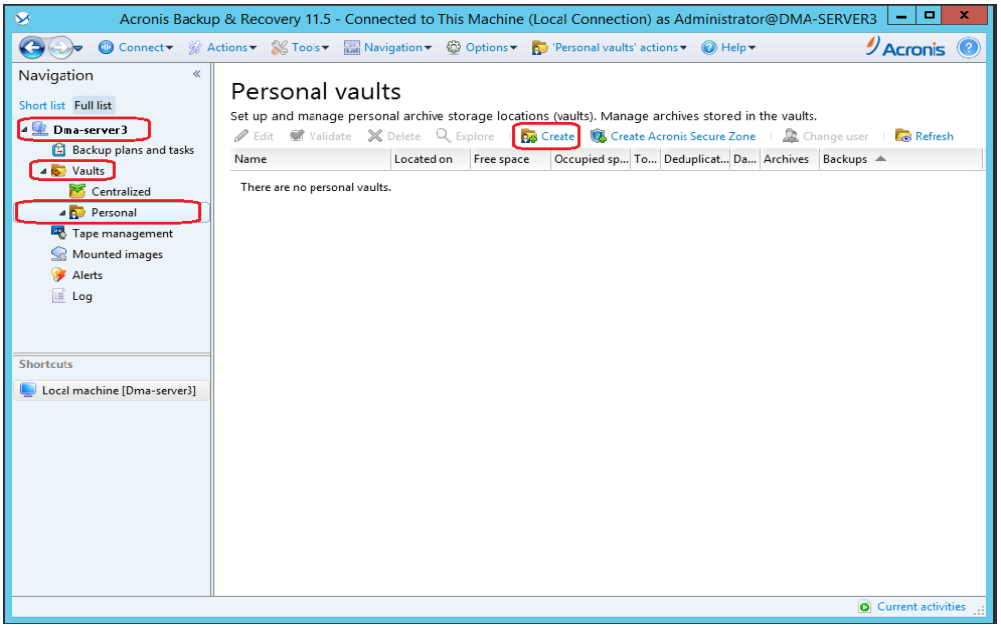
14 Review the summary and then click **Save** to add the container.

15 Confirm that the container is added.

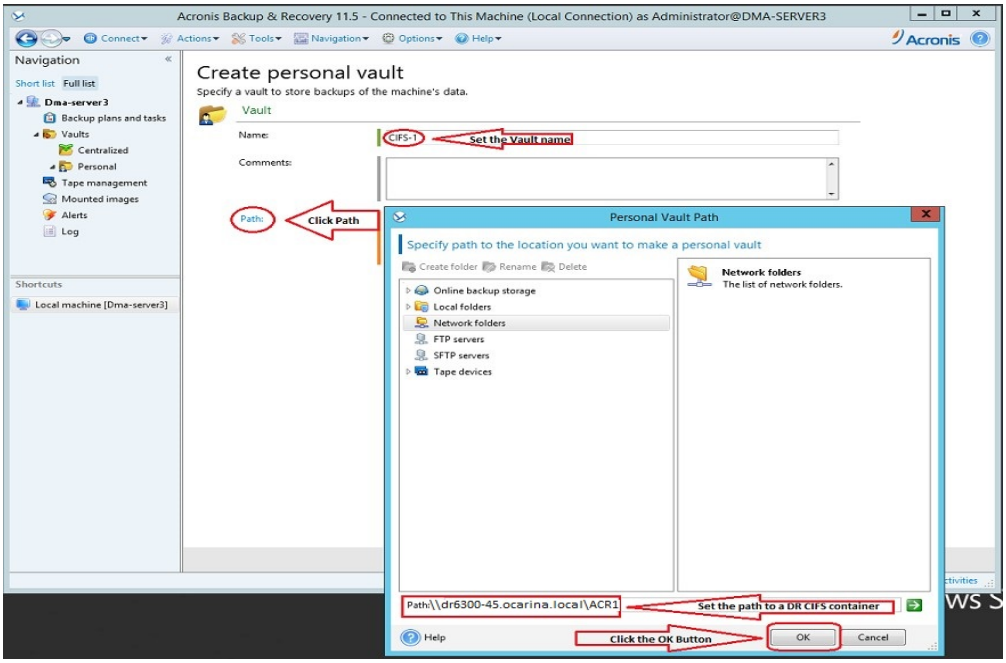
Setting up Acronis Backup & Recovery

For a Windows environment

1 Open Acronis Backup & Recovery Manager. Expand **Vaults --> Personal**, which displays the Acronis repositories and click on the **Create** Button.

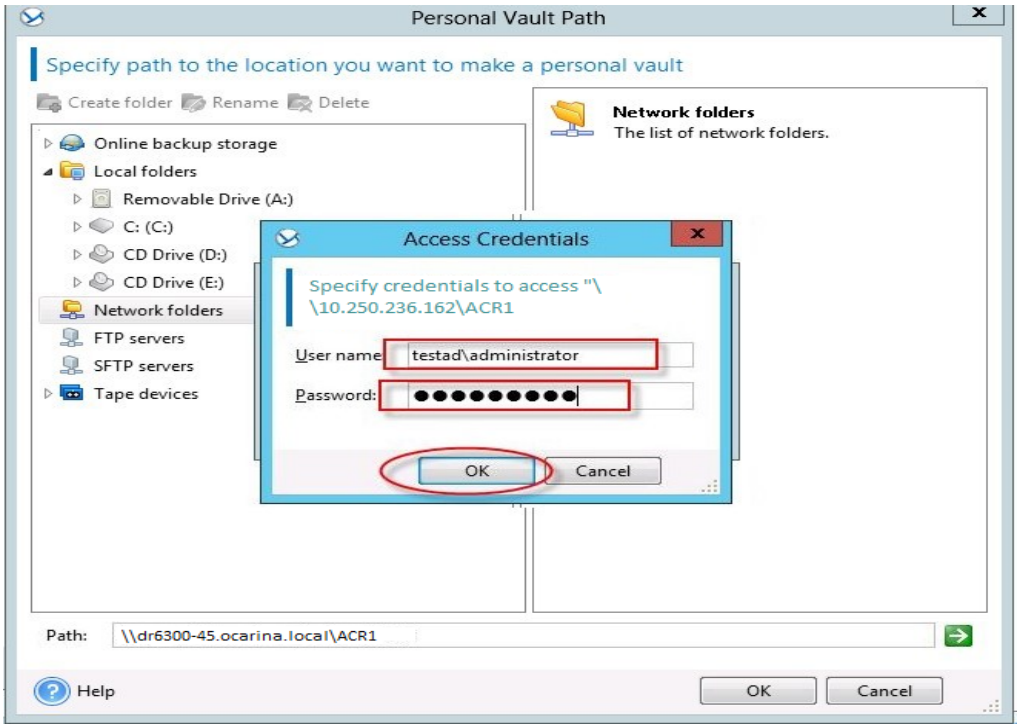


2 Specify the new vault **Name** that identifies the vault. Set the **Path** value to a Network folder which points to a DR CIFS container share, then click the **OK** button.

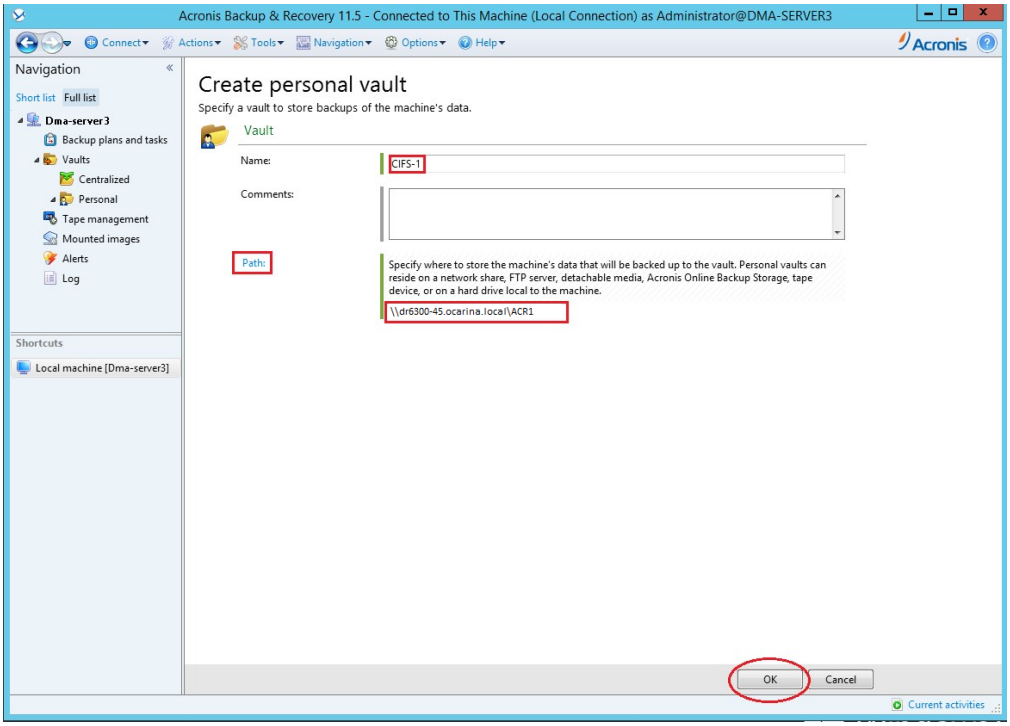


NOTE: The Windows service account for Acronis Backup & Recovery requires appropriate permissions to the DR Series Deduplication Appliance CIFS Share for the step below to complete successfully. See Appendix A for setting up the Acronis Backup & Recovery service account correctly. This should be done before the next step.

3 The next window asks for the credentials to access the CIFS share folder. Type in CIFS credential used for accessing the share, then click **OK**.



4 Click **OK** to finish vault creation.

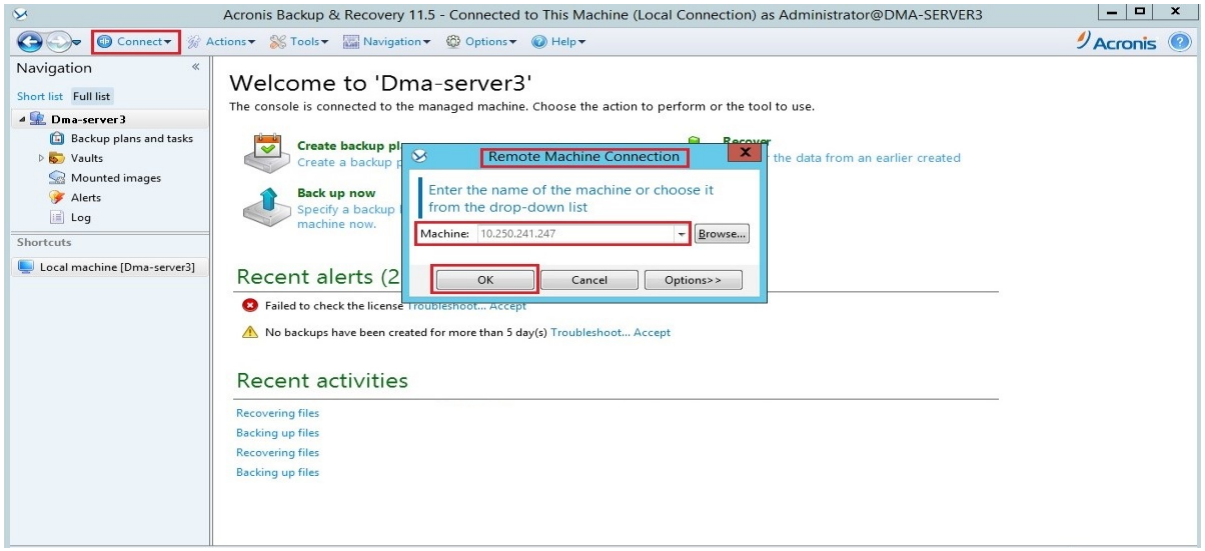


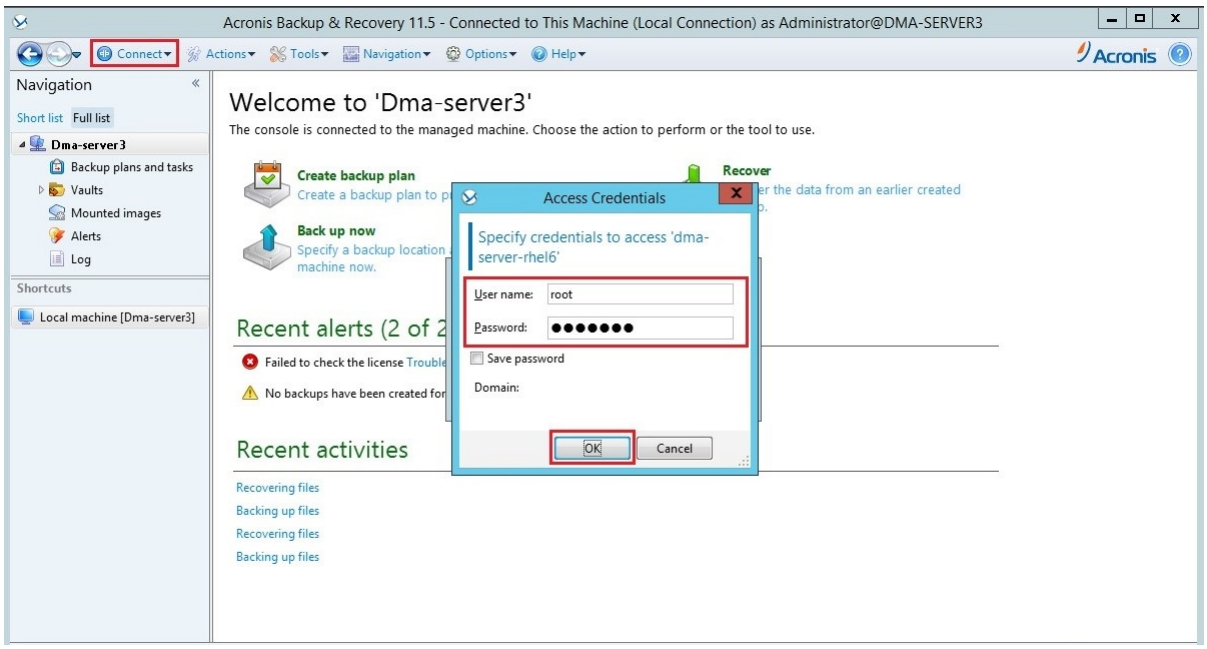
NOTE: Unlike other DMAs, Acronis B&R doesn't need the DR NFS share folder to be mounted on a client system.

For the Unix/Linux environment

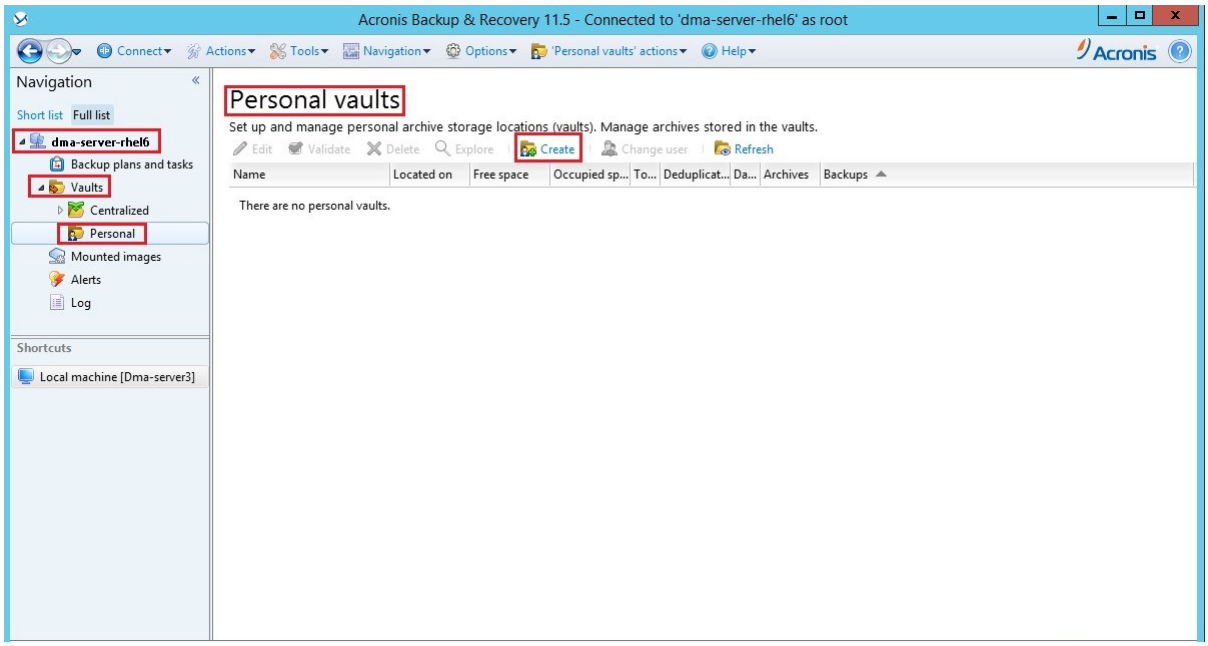
The procedure for the Unix/Linux Environment is very similar to the procedure for the Windows Environment. The only difference is that DR container NFS export path is used instead of a UNC path, as described below. For other details, please refer to 2.1 Procedure for the Windows Environment.

1 Open Acronis Backup & Recovery Manager, connect to an Acronis agent connect to an Acronis Linux agent by selecting **Connect → New connection → Manage a Remote Machine**. Enter the IP Address of the Linux client and enter access credentials

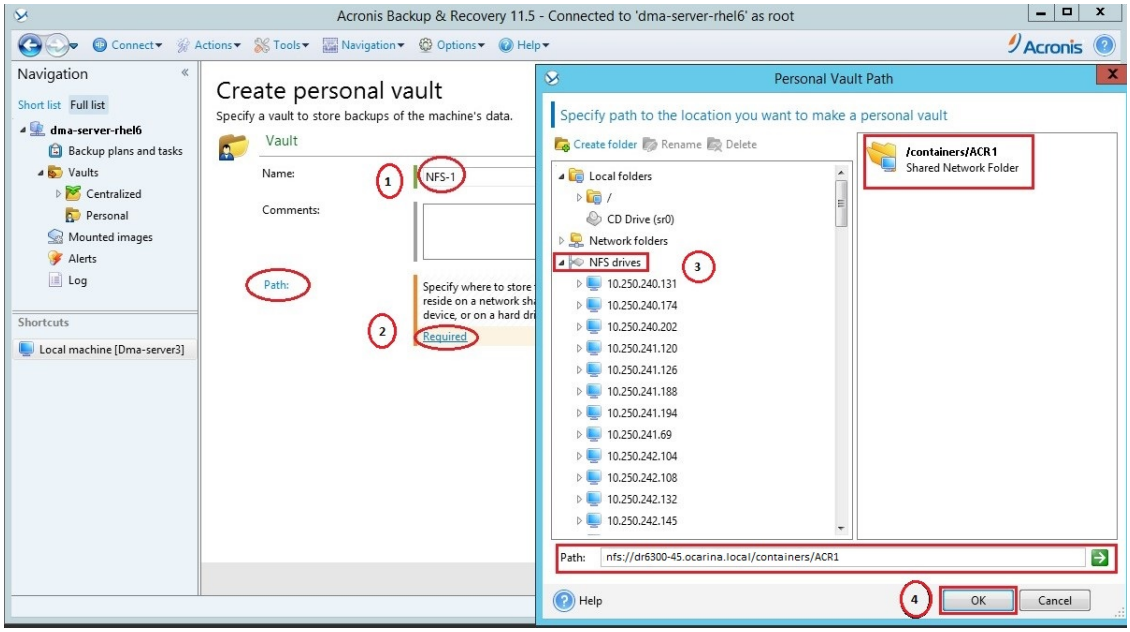

Acronis Backup & Recovery 11.5 - Connected to This Machine (Local Connection) as Administrator@DMA-SERVER3
Connect
Actions
Tools
Navigation
Options
Help
Acronis
Navigation
Short list
Full list
Dma-server3
Backup plans and tasks
Vaults
Mounted images
Alerts
Log
Shortcuts
Local machine [Dma-server3]
Welcome to 'Dma-server3'
The console is connected to the managed machine. Choose the action to perform or the tool to use.
Create backup pl
Create a backup
Back up now
Specify a backup
machine now.
Remote Machine Connection
Enter the name of the machine or choose it from the drop-down list
Machine:
10.250.241.247
Browse...
OK
Cancel
Options>>
Recent alerts (2
Failed to check the license
Troubleshoot... Accept
No backups have been created for more than 5 day(s)
Troubleshoot... Accept
Recent activities
Recovering files
Backing up files
Recovering files
Backing up files


Acronis Backup & Recovery 11.5 - Connected to This Machine (Local Connection) as Administrator@DMA-SERVER3
Connect
Actions
Tools
Navigation
Options
Help
Acronis
Navigation
Short list
Full list
Dma-server3
Backup plans and tasks
Vaults
Mounted images
Alerts
Log
Shortcuts
Local machine [Dma-server3]
Welcome to 'Dma-server3'
The console is connected to the managed machine. Choose the action to perform or the tool to use.
Create backup plan
Back up now
Specify a backup location
machine now.
Recover
Access Credentials
Specify credentials to access 'dma-server-rhel6'
User name:
root
Password:
Save password
Domain:
OK
Cancel
Recent alerts (2 of 2
Failed to check the license
No backups have been created for
Recent activities
Recovering files
Backing up files
Recovering files
Backing up files

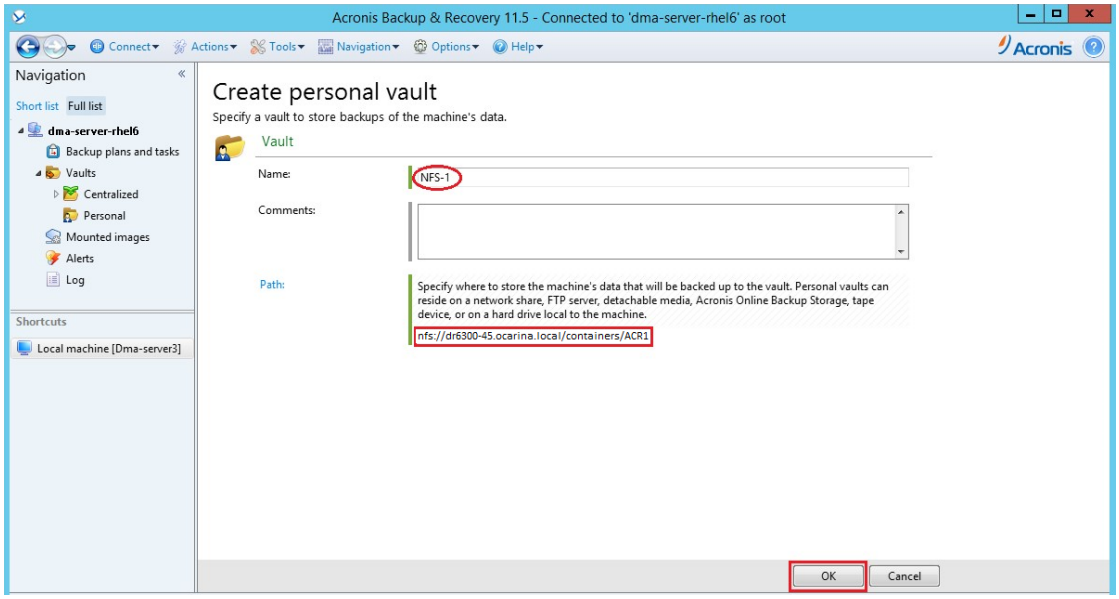
2 Expand **Vaults → Personal**, which displays the Acronis repositories, and click the **Create** icon.



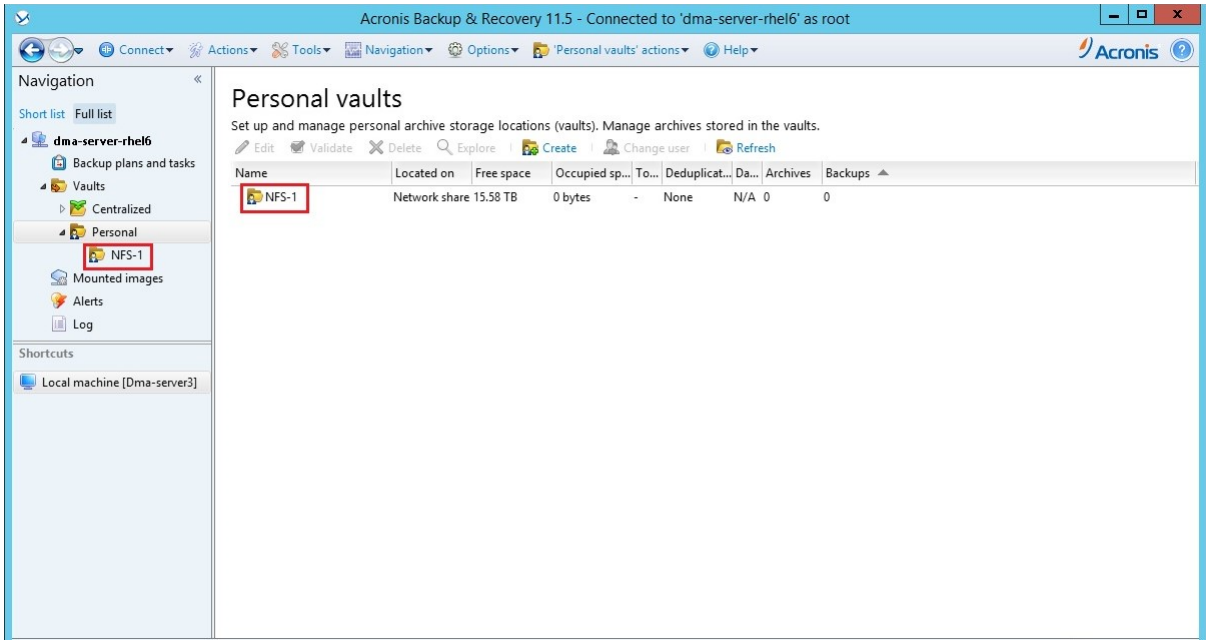
3 Specify the new vault **Name** that identifies the vault. Set the **Path** value to an NFS drive that points to a DR NFS container. Double-click the NFS share folder to add the folder to the Path value, and then click **OK**.



4 Click OK to finish the vault creation.

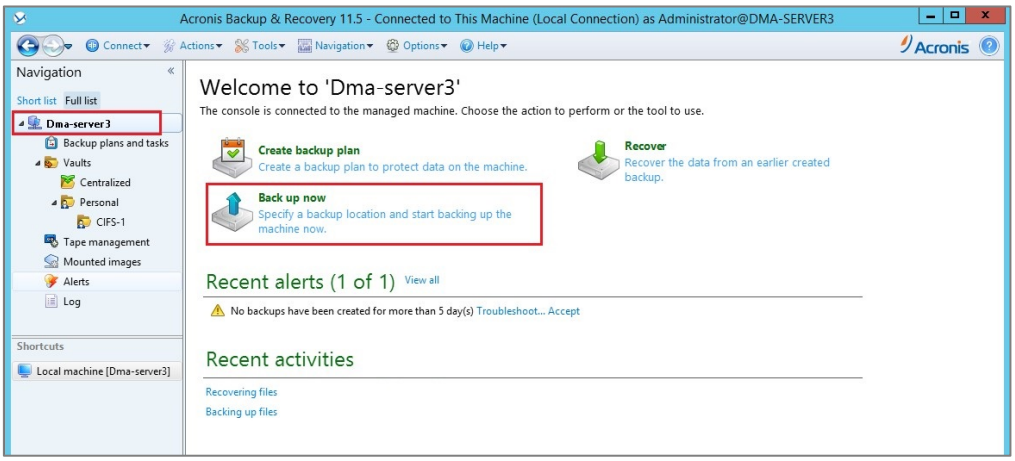


5 Finally verify the newly created vault information.

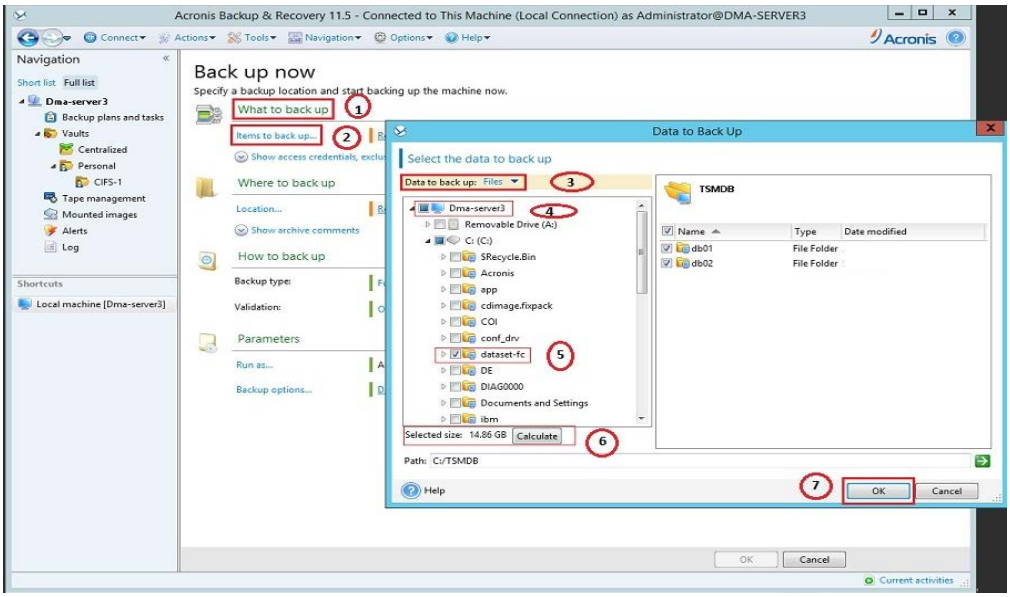

Acronis Backup & Recovery 11.5 - Connected to 'dma-server-rhel6' as root
Connect
Actions
Tools
Navigation
Options
'Personal vaults' actions
Help
Acronis
Navigation
Short list
Full list
dma-server-rhel6
Backup plans and tasks
Vaults
Centralized
Personal
NFS-1
Mounted images
Alerts
Log
Shortcuts
Local machine [Dma-server3]
Personal vaults
Set up and manage personal archive storage locations (vaults). Manage archives stored in the vaults.
Edit
Validate
Delete
Explore
Create
Change user
Refresh
Name
Located on
Free space
Occupied sp...
To...
Deduplicat...
Da...
Archives
Backups
NFS-1
Network share
15.58 TB
0 bytes
-
None
N/A
0
0

Creating a new backup job with the DR Series system as the backup target

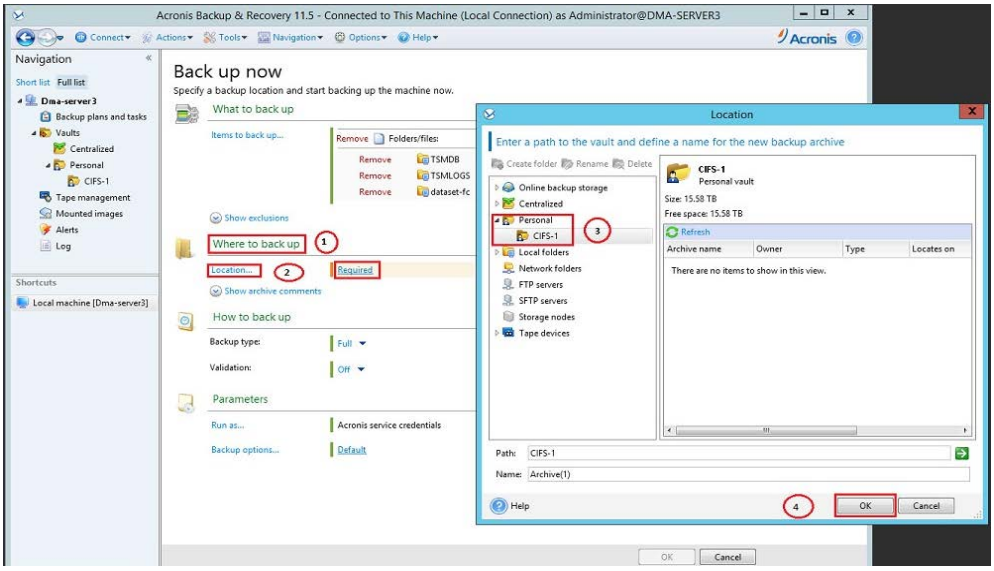
1 From Acronis B&R management console, click the DMA Server and then click **Back up now**.



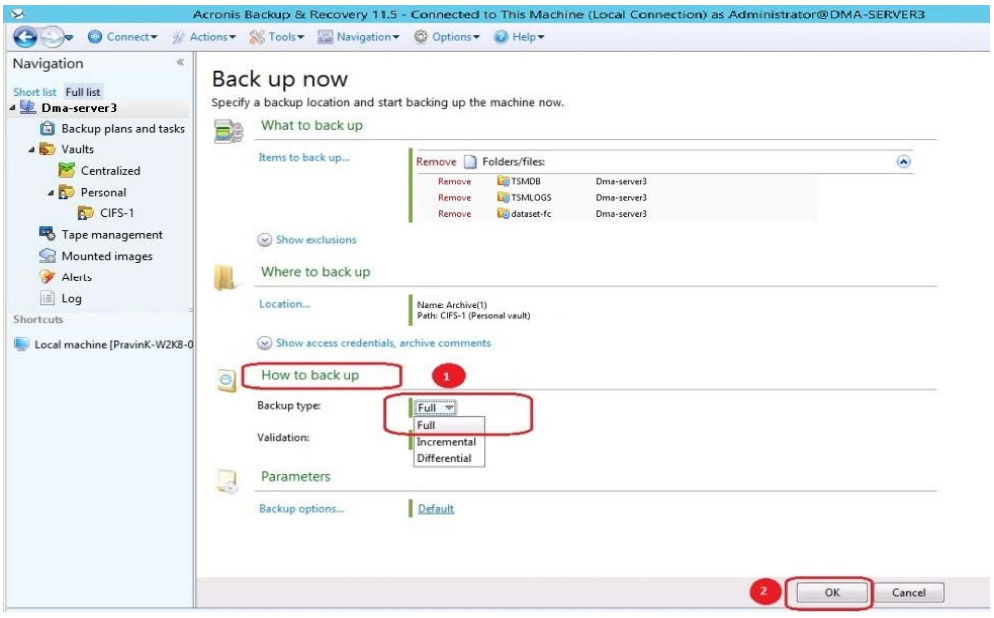
2 Under **What to backup**, click **Items to backup**, select a backup data set, and then click **OK.**



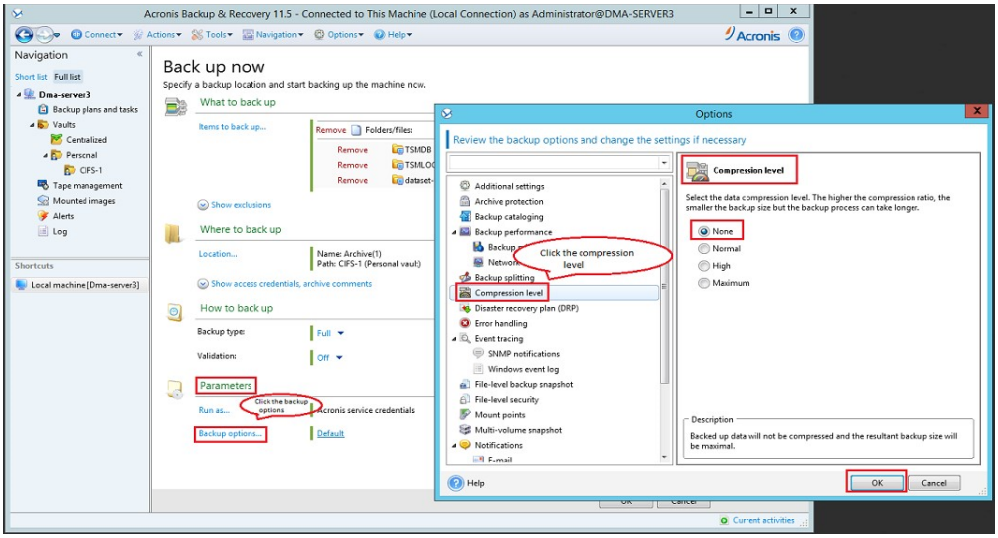
3 Under **Where to back up**, click **Location**, from **Personal** folder, select the vault that points to the DR CIFS or NFS container, and click **OK**.



4 Under **How to back up**, define the **Backup type** and **Validation**, and click **OK**.

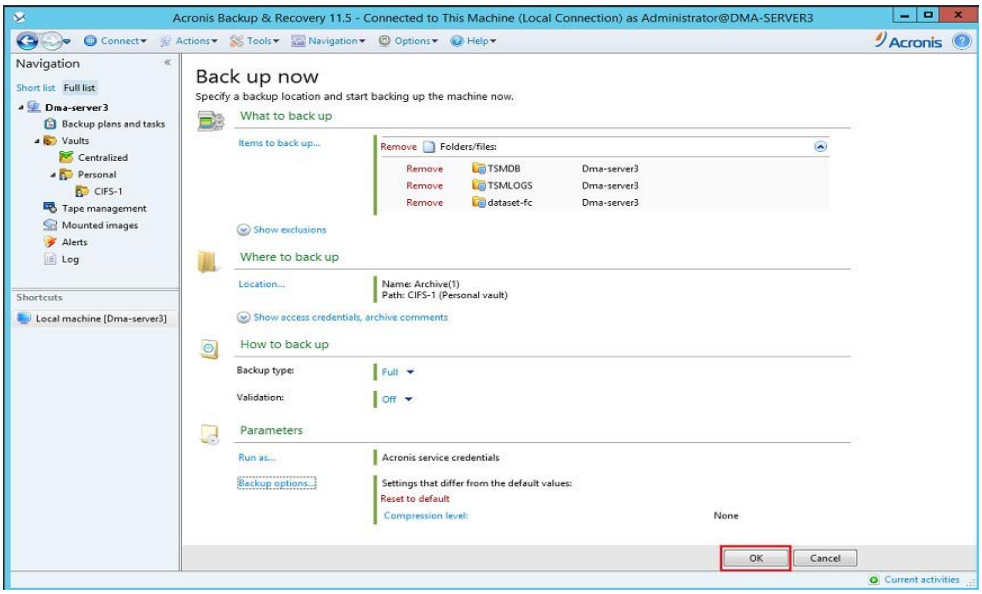


5 Under **Parameters**, click **Backup options**, and, in the **Options** window, **click Compression level**, select **None** and click **OK**.

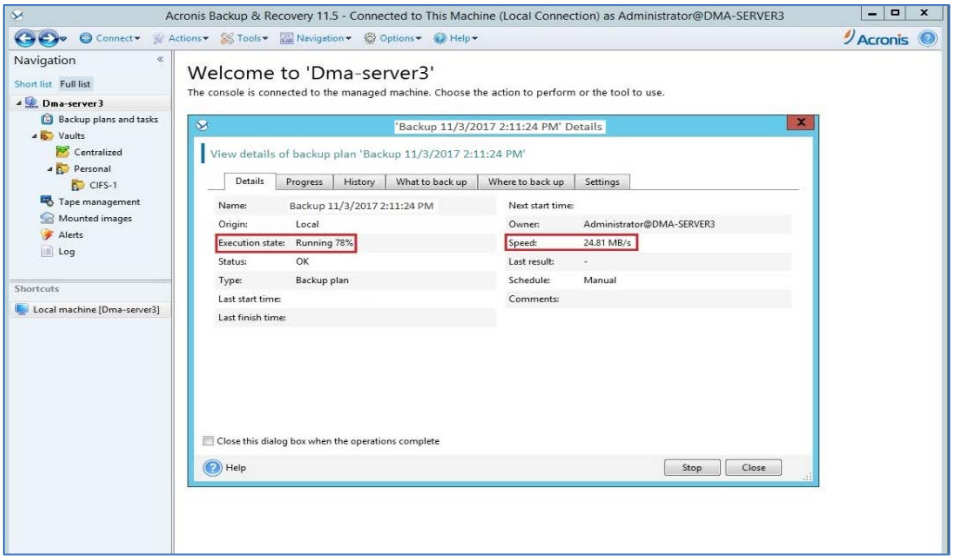


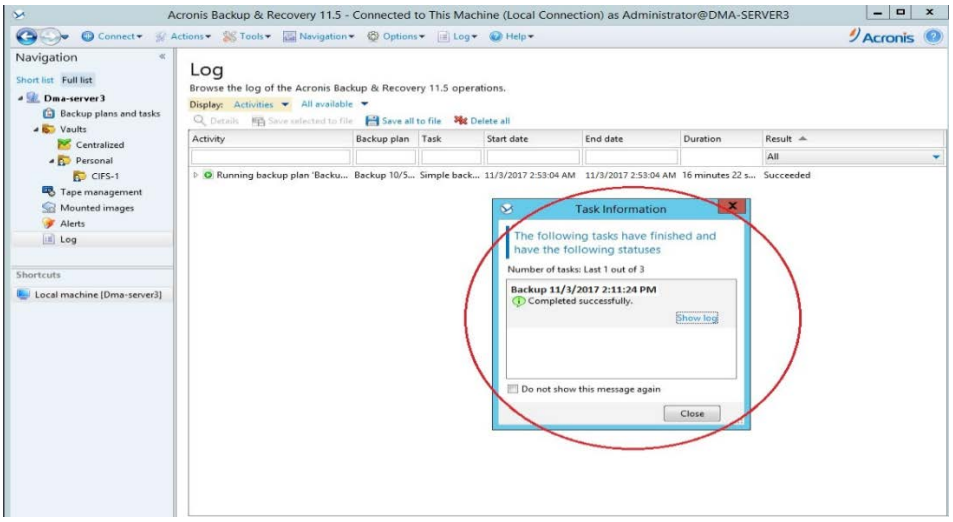
NOTE: Always Disable 'Software compression', as the DR Series system has compression built-in and does not require compression on Acronis Backup & Recovery. In general, additional data compression on backup software will have a negative impact on total savings on the DR Series system. Set Data security to **none**, as enabling encryption before the data stream is sent to the DR Series system will make the data unable to be de-duplicated. This will have a significant, negative impact on total savings on the DR Series system.

6 Click **OK** to save the newly configured backup specification.



7 The backup job will run based on the defined schedule. You can monitor backup job progress on the Details tab. Once it is finished, the backup job run result window opens.


Acronis Backup & Recovery 11.5 - Connected to This Machine (Local Connection) as Administrator@DMA-SERVER3
Connect
Actions
Tools
Navigation
Options
Help
Acronis
Navigation
Short list
Full list
Dma-server3
Backup plans and tasks
Vaults
Centralized
Personal
CIFS-1
Tape management
Mounted images
Alerts
Log
Shortcuts
Local machine [Dma-server3]
Welcome to 'Dma-server3'
The console is connected to the managed machine. Choose the action to perform or the tool to use.
'Backup 11/3/2017 2:11:24 PM' Details
View details of backup plan 'Backup 11/3/2017 2:11:24 PM'
Details
Progress
History
What to back up
Where to back up
Settings
Name: Backup 11/3/2017 2:11:24 PM
Origin: Local
Execution state: Running 78%
Status: OK
Type: Backup plan
Last start time:
Last finish time:
Next start time:
Owner: Administrator@DMA-SERVER3
Speed: 24.81 MB/s
Last result: -
Schedule: Manual
Comments:
Close this dialog box when the operations complete
Help
Stop
Close


Acronis Backup & Recovery 11.5 - Connected to This Machine (Local Connection) as Administrator@DMA-SERVER3
Connect
Actions
Tools
Navigation
Options
Log
Help
Acronis
Navigation
Short list
Full list
Dma-server3
Backup plans and tasks
Vaults
Centralized
Personal
CIFS-1
Tape management
Mounted images
Alerts
Log
Shortcuts
Local machine [Dma-server3]
Log
Browse the log of the Acronis Backup & Recovery 11.5 operations.
Display: Activities
All available
Details
Save selected to file
Save all to file
Delete all
Activity
Backup plan
Task
Start date
End date
Duration
Result
All
Running backup plan 'Backu...
Backup 10/S...
Simple back...
11/3/2017 2:53:04 AM
11/3/2017 2:53:04 AM
16 minutes 22 s...
Succeeded
Task Information
The following tasks have finished and have the following statuses
Number of tasks: Last 1 out of 3
Backup 11/3/2017 2:11:24 PM
Completed successfully.
Show log
Do not show this message again
Close

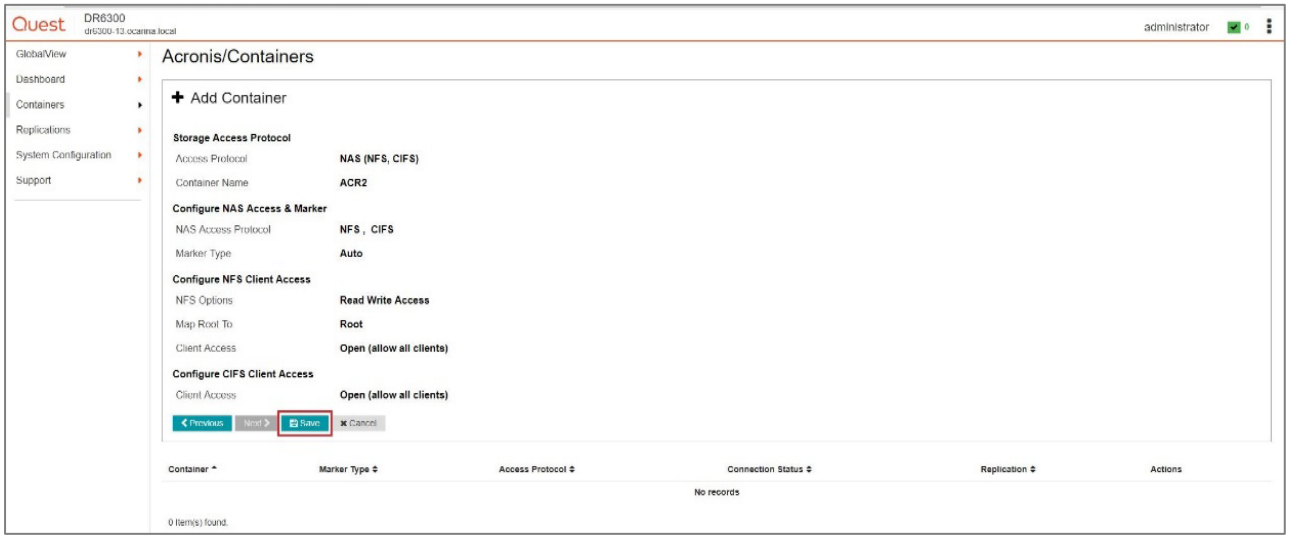
4

Setting up DR native replication & restore from a replication target DR

Creating a DR native replication session

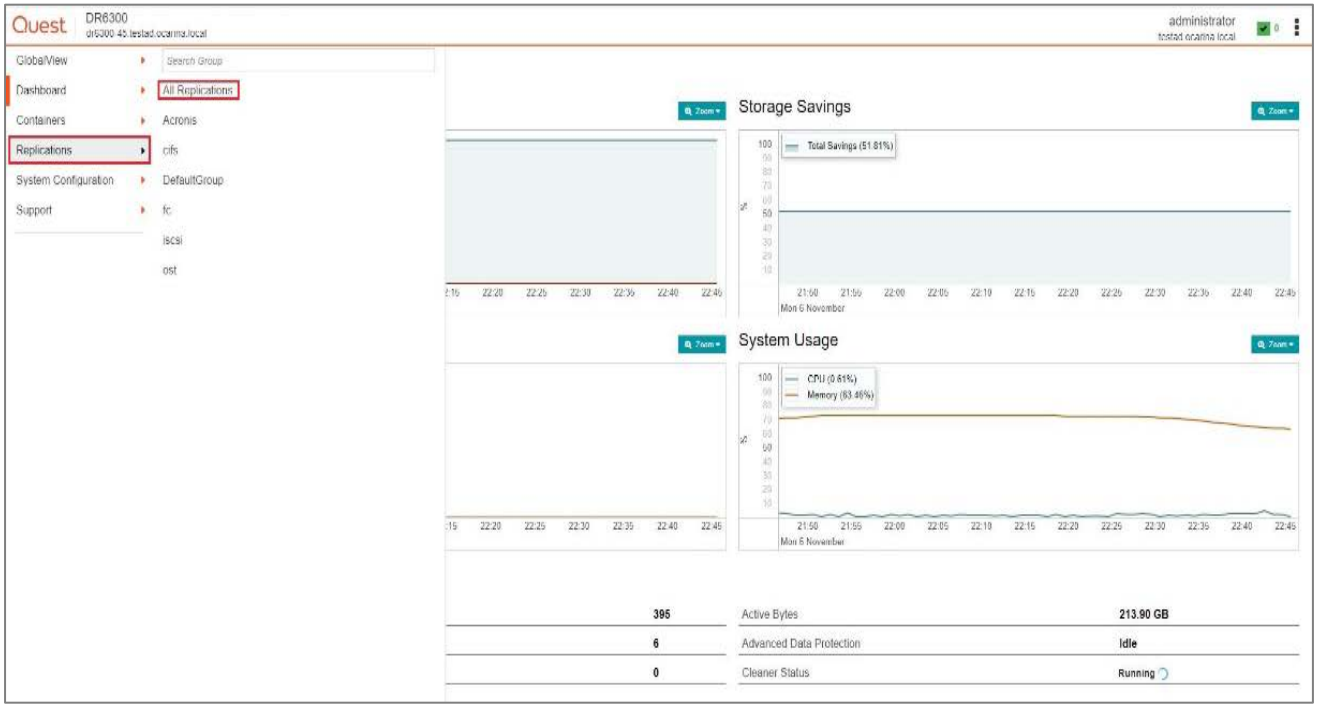
1 In the replication target DR Series system GUI, create a container by selecting **Containers** in the left navigation menu, and then, on the Actions menu, clicking **Add Container**.

2 Enter the required container information.

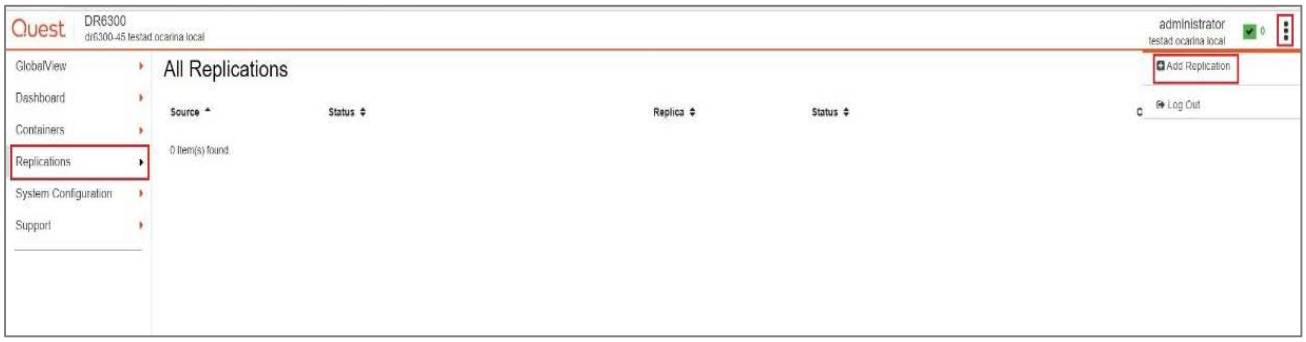


3 Click the **Save** button to create a new container on the target DR Series system.

4 Go back to the source DR Series system, select **Replication** from the left navigation menu, and click **All Replications**.

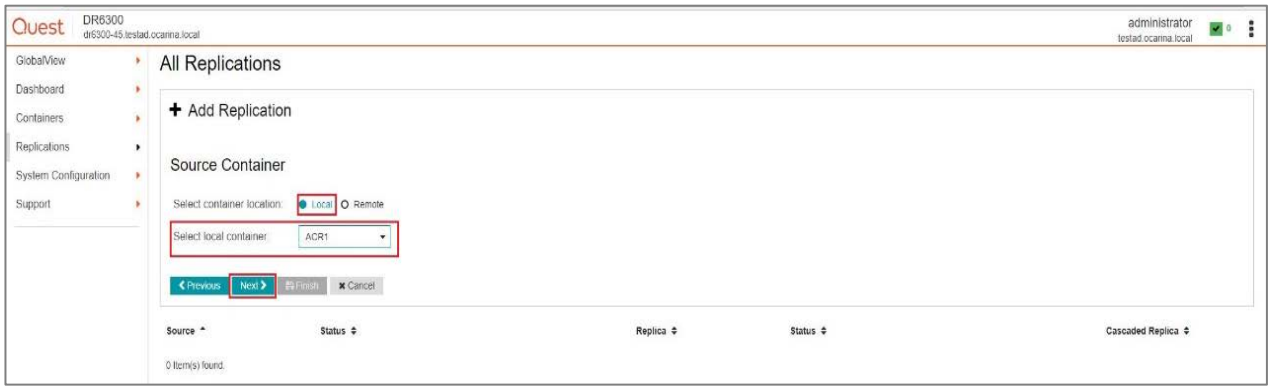


5 On the Actions menu in the upper right corner of the page, click **Add Replication**.



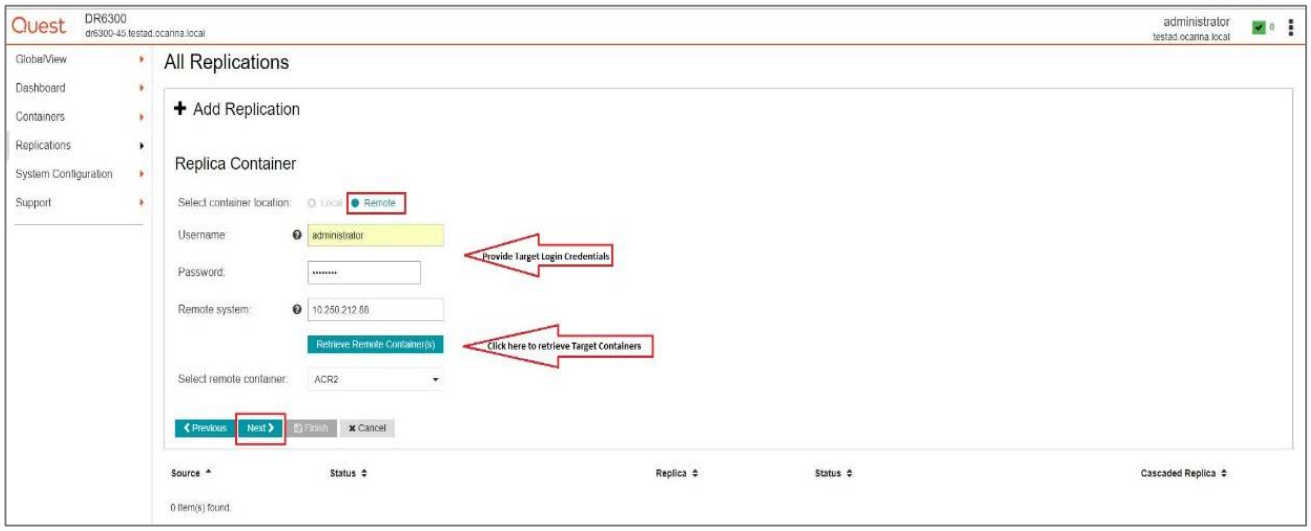
6 Choose the Replication Type as **Replica only** and click the **Next** button.

7 Select the source container location as **Local**, select the container from the drop-down menu, and then click the **Next** button.

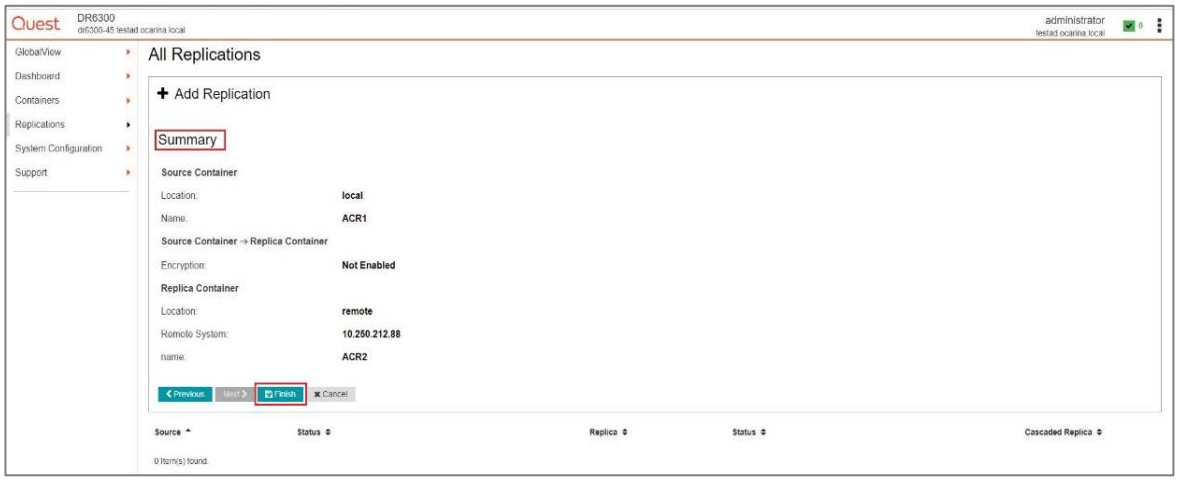


8 Select the Encryption type as needed.

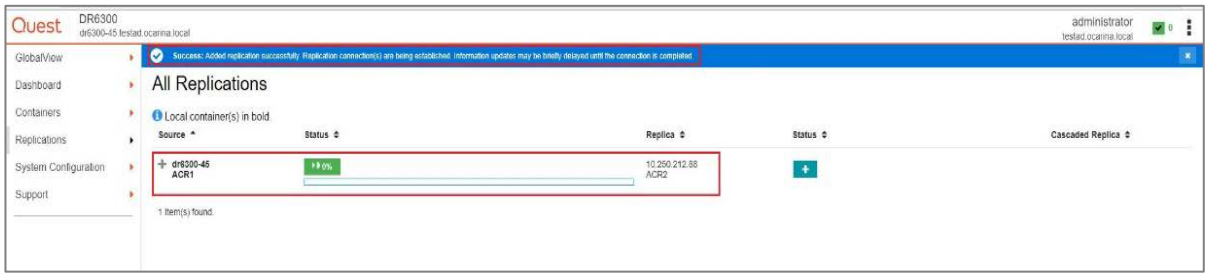
9 Enter the remote DR Series system credentials (Admin Username, Password and target DR IP Address), click **Retrieve the Remote Container(s)**, select the target container, and click the **Next** button.



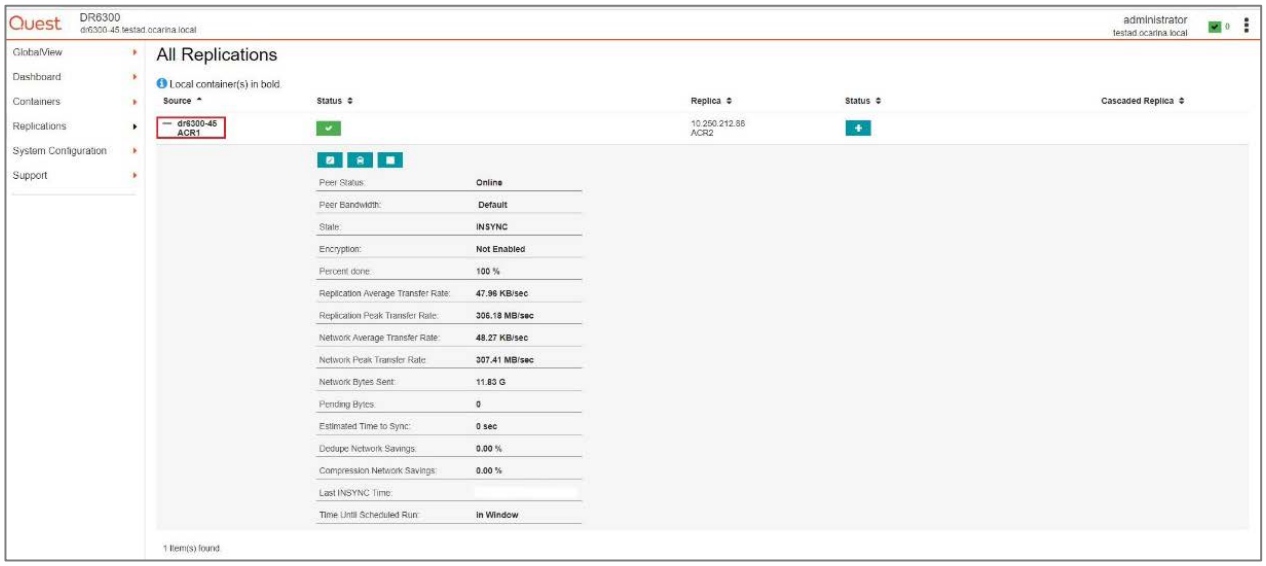
10 Verify the summary and click **Finish** to establish replication between the source and target containers.



11 Verify that Replication is established successfully between the source and target containers.



12 Click the **+ icon** on the left side of the replication pair to view replication statistics.



Restoring from the replication target

There are two ways to restore from a replication target:

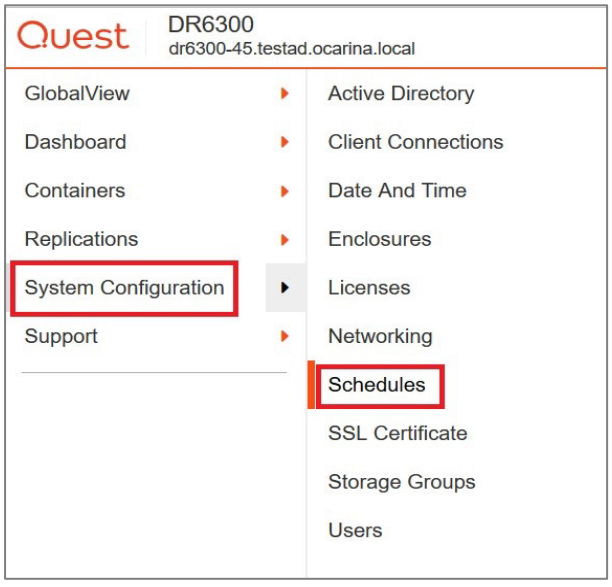
- Replication Target as imported repository:
  - a Add the replication target DR container share/export into the Acronis **Vault** under **Personal folder**. Please refer to **Section 2** of this document for detailed instructions.
  - b Select the backup set from the target DR container, and restore from it.
- Update replication target DR to have same hostname/IP as replication source
  - a Update replication **target DR hostname** and/or **IP** the same as the replication source DR
    - If both the DR appliances are joined into the Active Directory domain, both of them need to be removed from the Active directory domain first.
    - Next, update the target DR hostname/IP.
    - Finally, re-join the system into the Active directory domain.
  - b Select the backup set from the DR container, and restore from it.

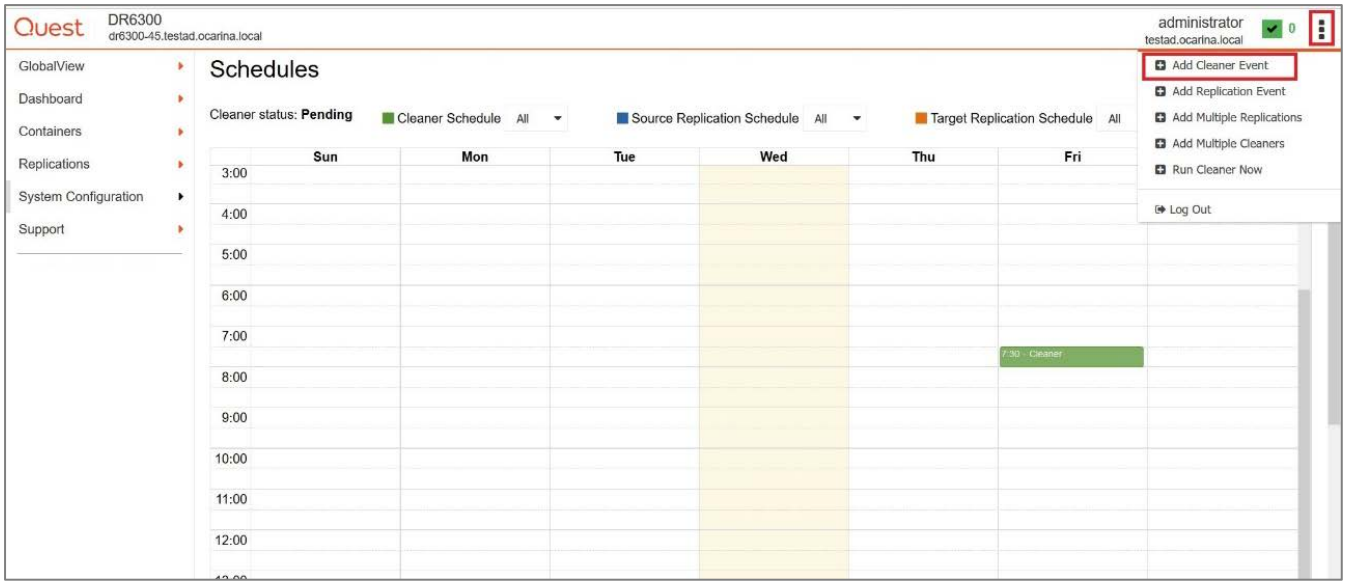
Setting up the DR Series system cleaner

The cleaner will run 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 which will force it to run during that scheduled time.

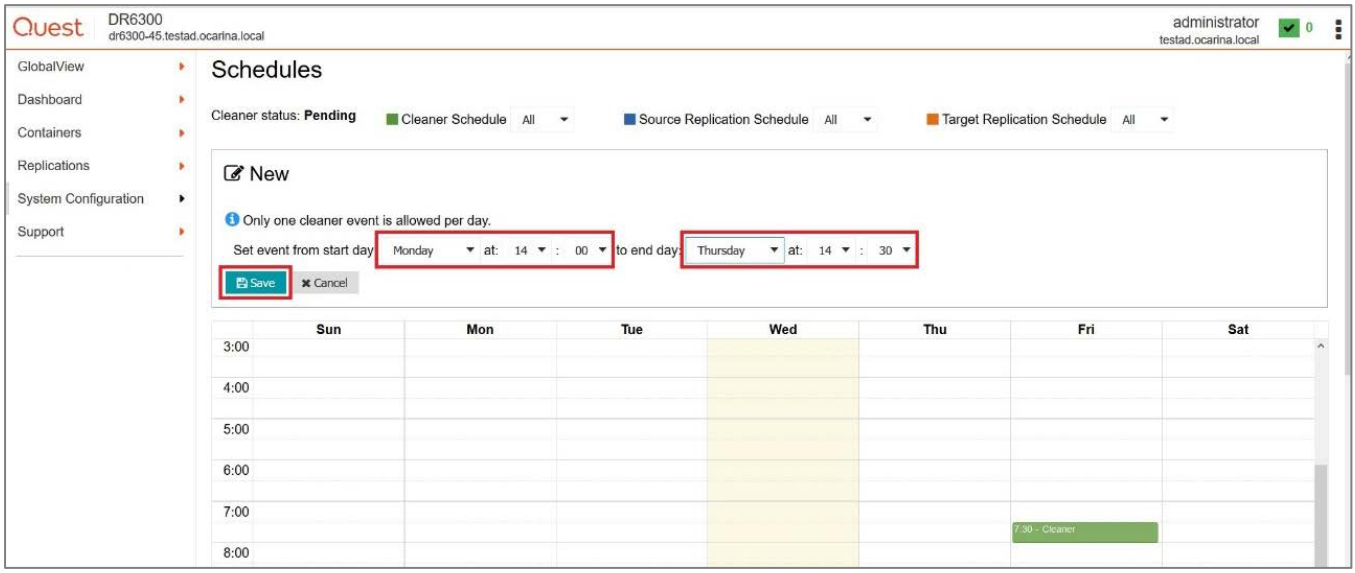
If necessary, you can do the following procedure as described in the screenshot to force the cleaner to run. Once all the backup jobs are set up the DR Series system cleaner can be scheduled. The system cleaner should run at least 40 hours per week when backups are not taking place, generally after a backup job has completed.

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.





You can create a cleaner schedule as shown below.



6

Monitoring deduplication, compression and performance

After backup jobs have completed, the DR Series system tracks capacity, storage savings and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits 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 complete, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio in most cases.