Quest™

Setting up the DR Series system as a CIFS and NFS target on CA ArcServe v16.5

Technical White Paper

Quest Engineering

October 2017

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 OFANY KIND

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

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.**

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

Setting Up the DR Series System as a CIFS and NFS Target on CA ArcServe v16.5

Updated – December 20, 2017

Contents

Installing and configuring the DR Series system 6

Creating a disk-based target device on CA ARCserve 13

For the Windows environment 13

For the Unix/Linux environment 15

Creating a new backup job with the DR Series system as the target 17

Setting up DR native replication & restoring from a replication target 22

Creating a DR Series replication session 22

Restoring from the replication target 26

Setting up the system cleaner 30

Monitoring deduplication, compression and performance 32

Appendices 33

A - Creating a storage device for NFS 33

Revisions

Date	Description
January 2014	Initial release
November 2016	Updated the guide with new DR-4.0 GUI screens
October 2017	Updated with new Quest branded DR Series system GUI (v4.0.3)

Executive Summary

This document provides information about how to set up the DR Series system as a backup target for CA ArcServe v16.5.

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 CA ArcServe, refer to the ArcServe documentation at:

https://documentation.arcserve.com/Arcserve-Backup/Available/R16/ENU/bookshelf.html

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

Installing and configuring the DR Series system

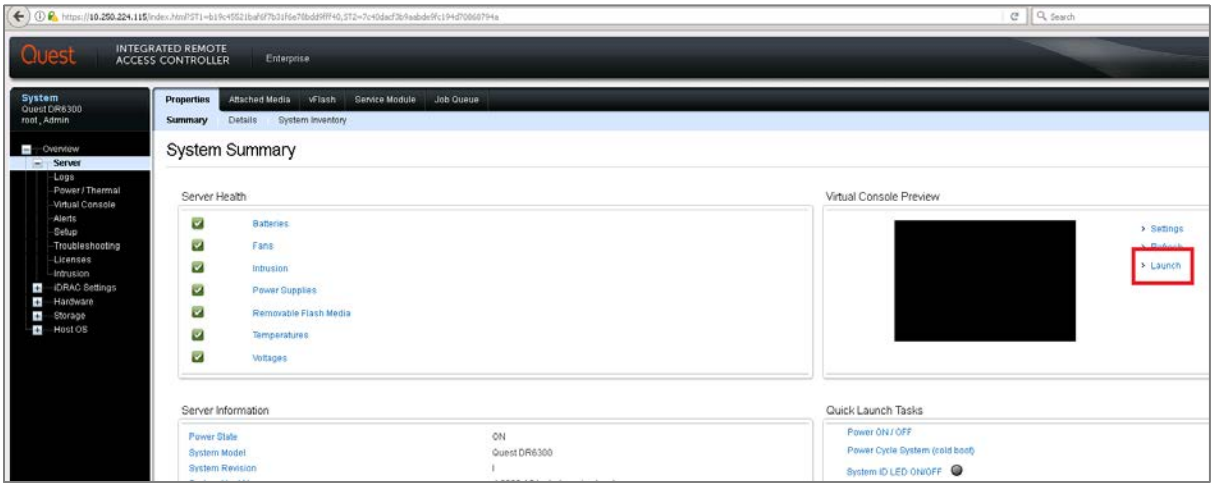
1 Rack and cable the DR Series system, and power it on. In the *Quest DR Series System Administrator Guide*, see the following sections for information about using the iDRAC connection and initializing the appliance.

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

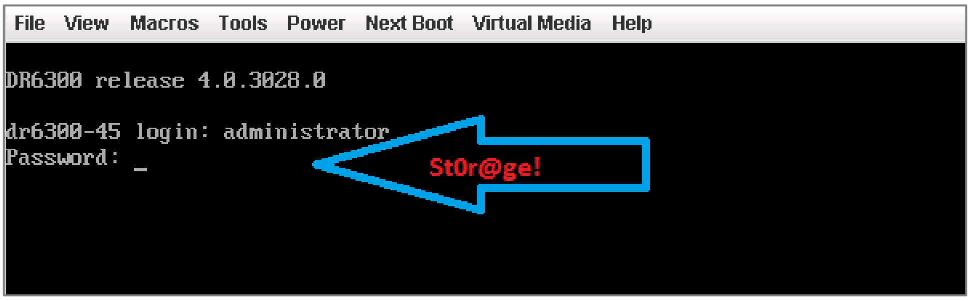
2 Log on to iDRAC using the default credentials (username: **root** and password: **calvin**) and either:

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

3 Launch the virtual console.

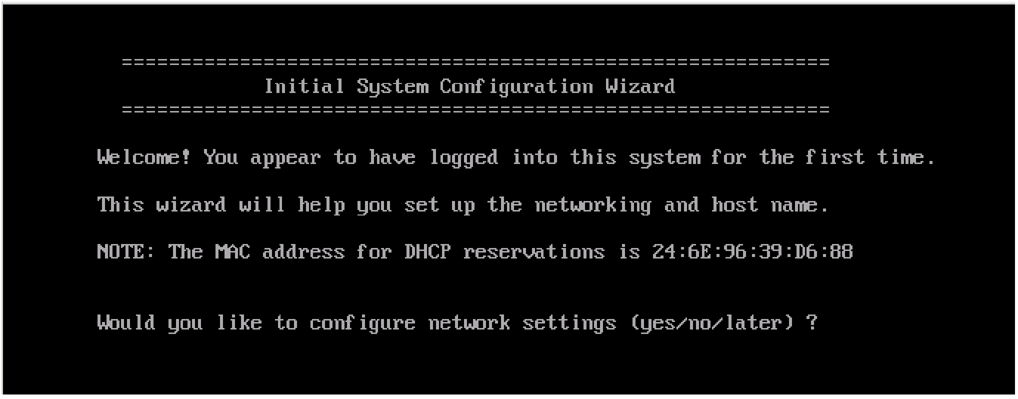


4 After the virtual console opens, log on to the system (with the username: **administrator** and password: **St0r@ge!** where the "0" in the password is the numeral zero).



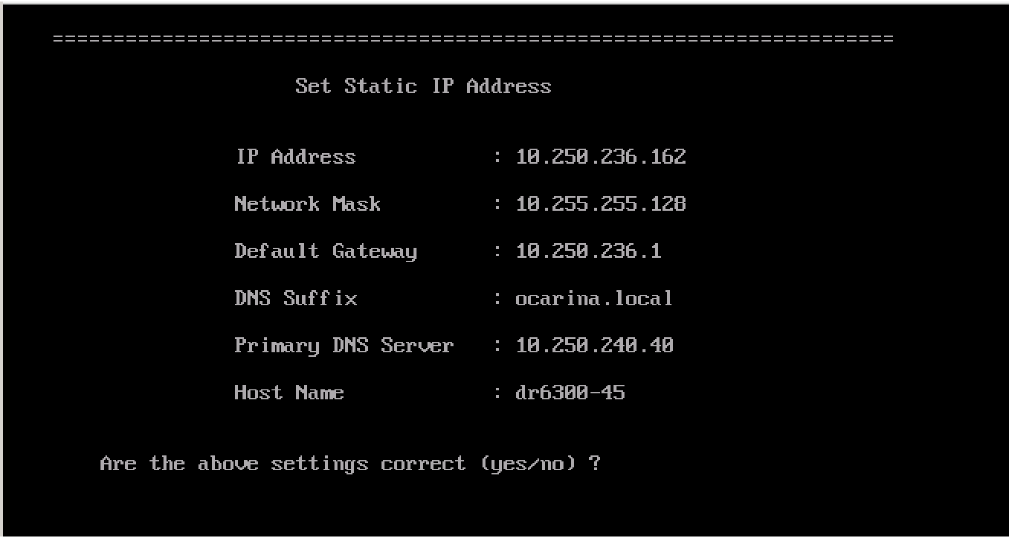
```
DR6300 release 4.0.3028.0

dr6300-45 login: administrator
Password: _
```

5 Set the user-defined networking preferences.



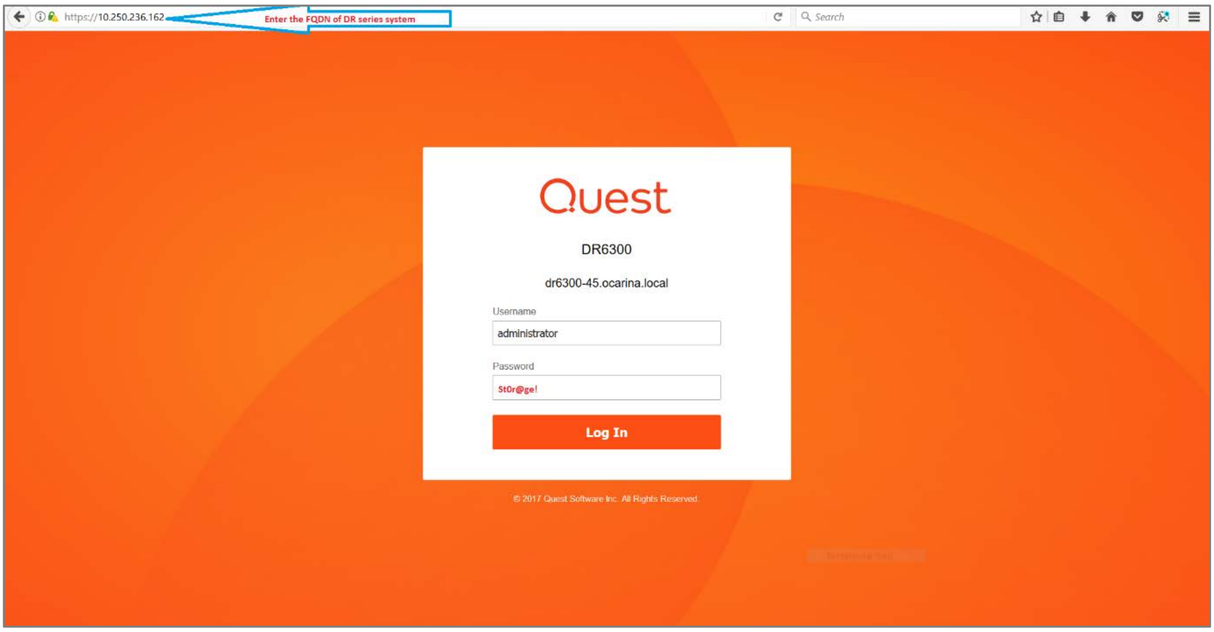
```
      ============================================================
                  Initial System Configuration Wizard
      ============================================================

    Welcome! You appear to have logged into this system for the first time.

    This wizard will help you set up the networking and host name.

    NOTE: The MAC address for DHCP reservations is 24:6E:96:39:D6:88


    Would you like to configure network settings (yes/no/later) ?
```

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



```
  ========================================================================

                       Set Static IP Address


                  IP Address            : 10.250.236.162

                  Network Mask          : 10.255.255.128

                  Default Gateway       : 10.250.236.1

                  DNS Suffix            : ocarina.local

                  Primary DNS Server    : 10.250.240.40

                  Host Name             : dr6300-45


      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@ge!** (The "0" in the password is the numeral zero.).



https://10.250.236.162

Enter the FQDN of DR series system

DR6300

dr6300-45.ocarina.local

Username: administrator

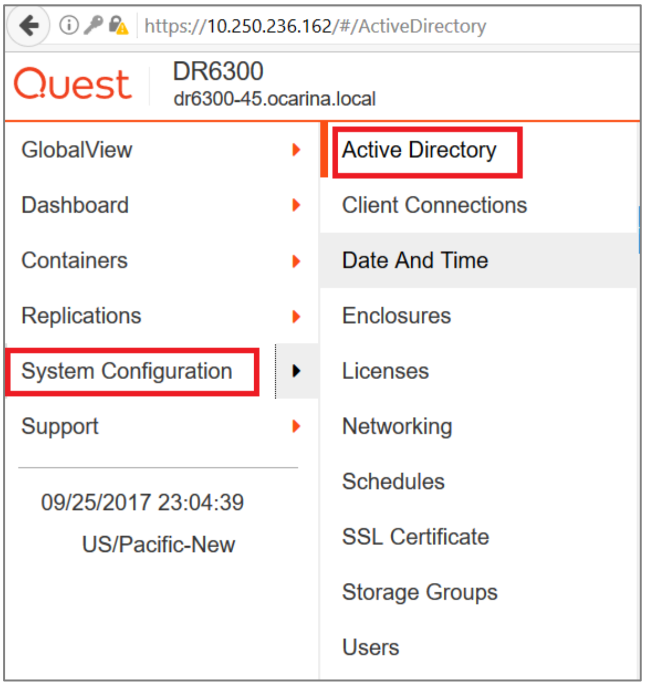
Password: St0r@ge!

© 2017 Quest Software Inc. All Rights Reserved.

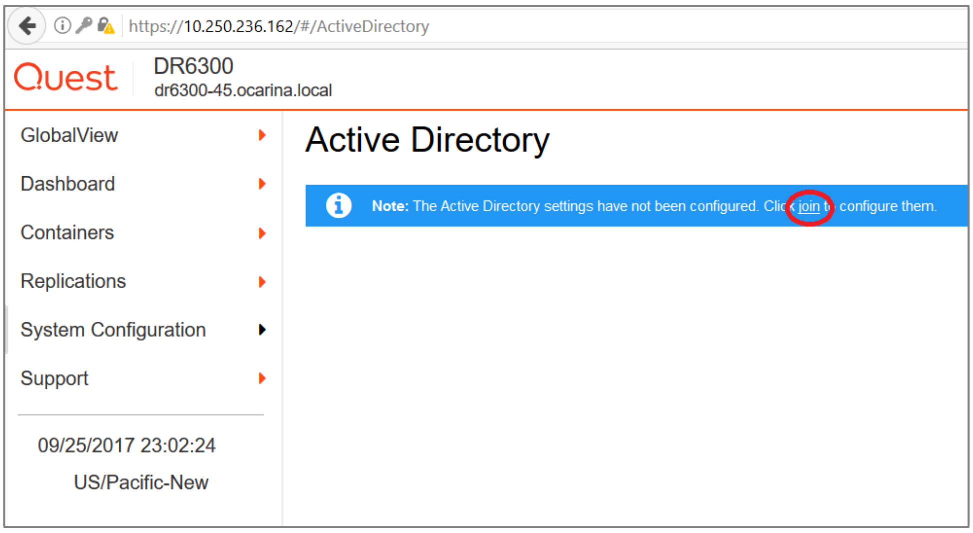
8 Join the DR Series system to Active Directory.

> 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**.



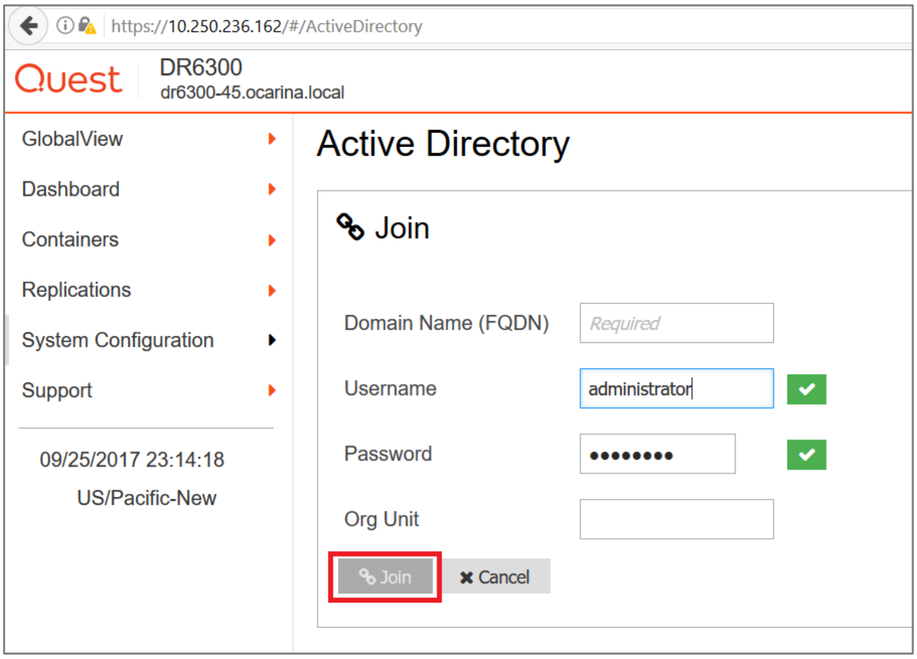
b Click **Join**.



Active Directory

Note: The Active Directory settings have not been configured. Click join to configure them.

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



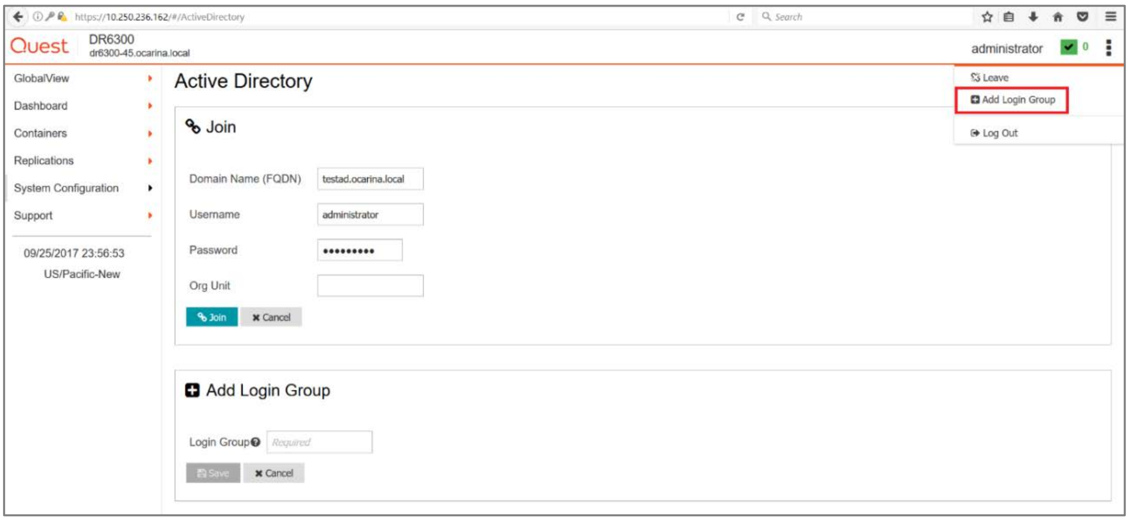
Domain Name (FQDN): Required

Username: administrator ✓

Password: •••••••• ✓

Org Unit:

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



Domain Name (FQDN): testad.ocarina.local

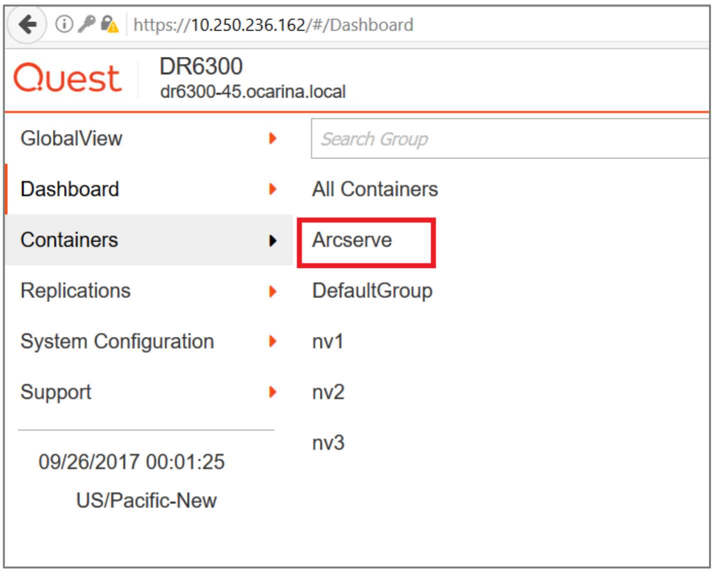
Username: administrator

Password: •••••••••

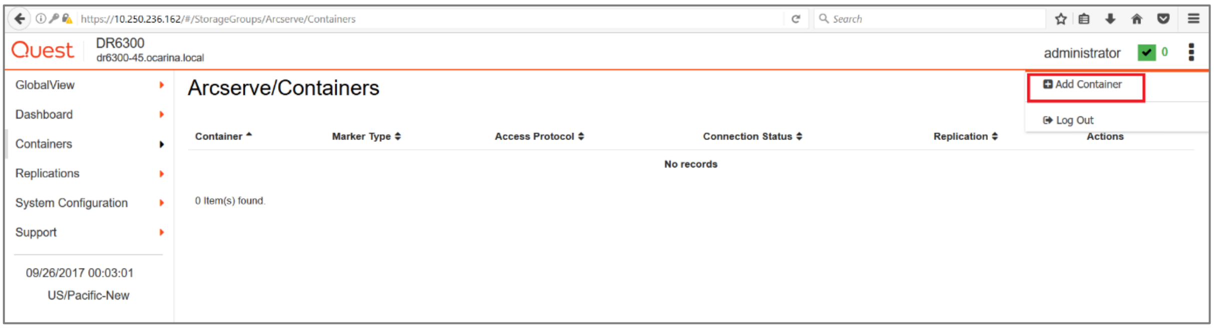
Org Unit:

Login Group: Required

9 You now need to create and mount the container. In the left navigation menu, click **Containers -> <Storage Group>.**

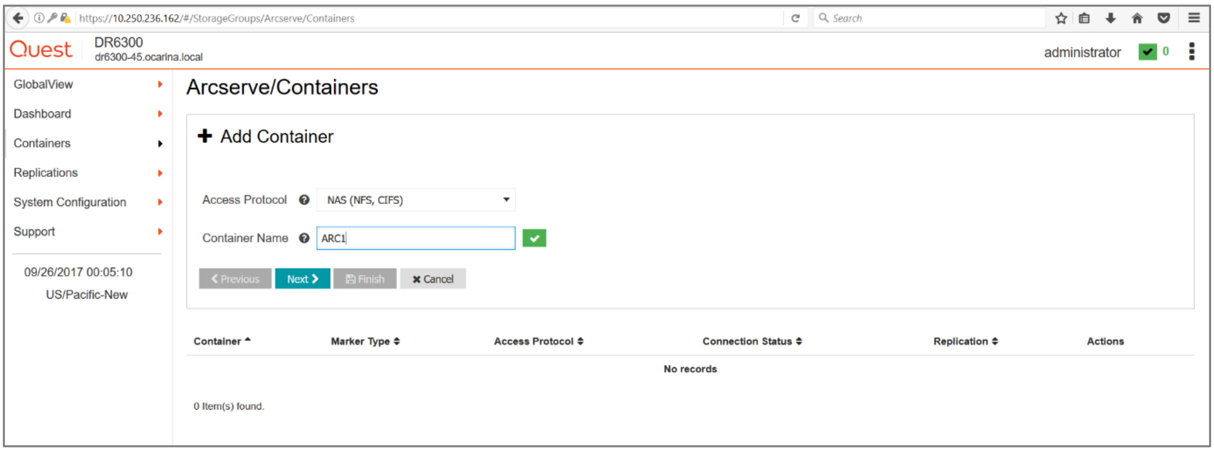


10 On the Action menu in the upper right corner of the page, **Add Container**.



11 Enter a container name.

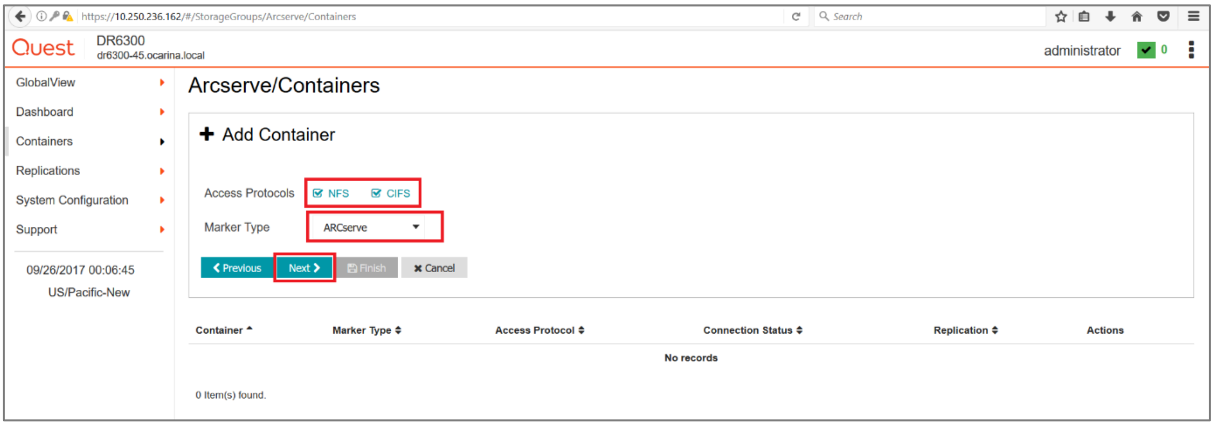
12 For the Access Protocol, select **NAS (NFS, CIFS)** and then click **Next**.



Access Protocol: NAS (NFS, CIFS)

Container Name: ARC1

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



Arcserve/Containers

Add Container

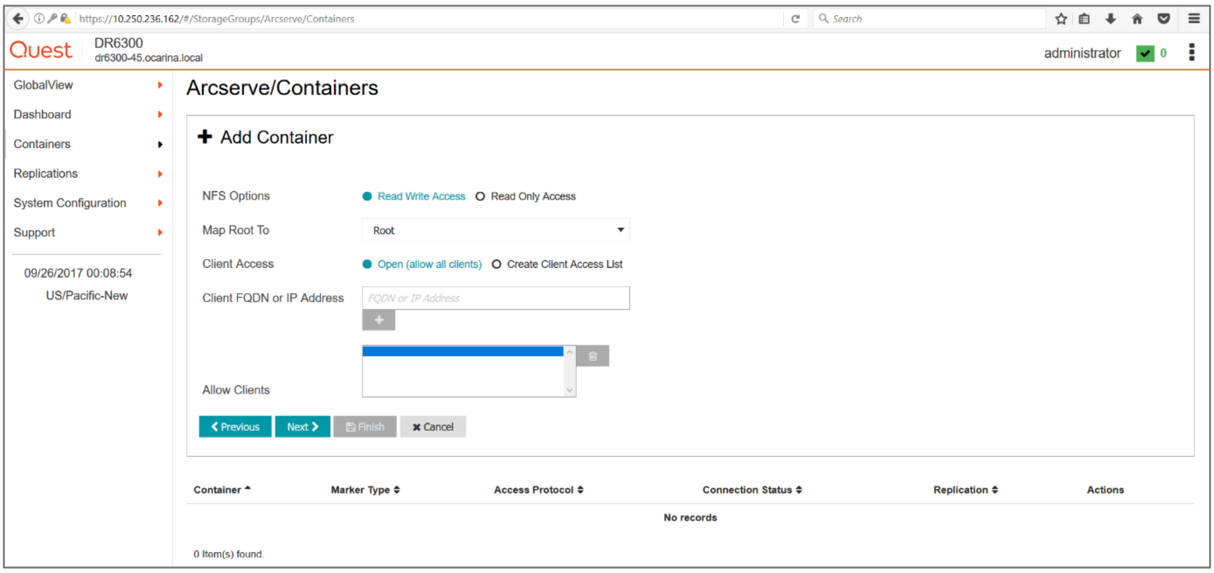
Access Protocols ☑ NFS ☑ CIFS

Marker Type ARCserve

Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
No records					

0 Item(s) found.

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



Arcserve/Containers

Add Container

NFS Options ● Read Write Access ○ Read Only Access

Map Root To Root

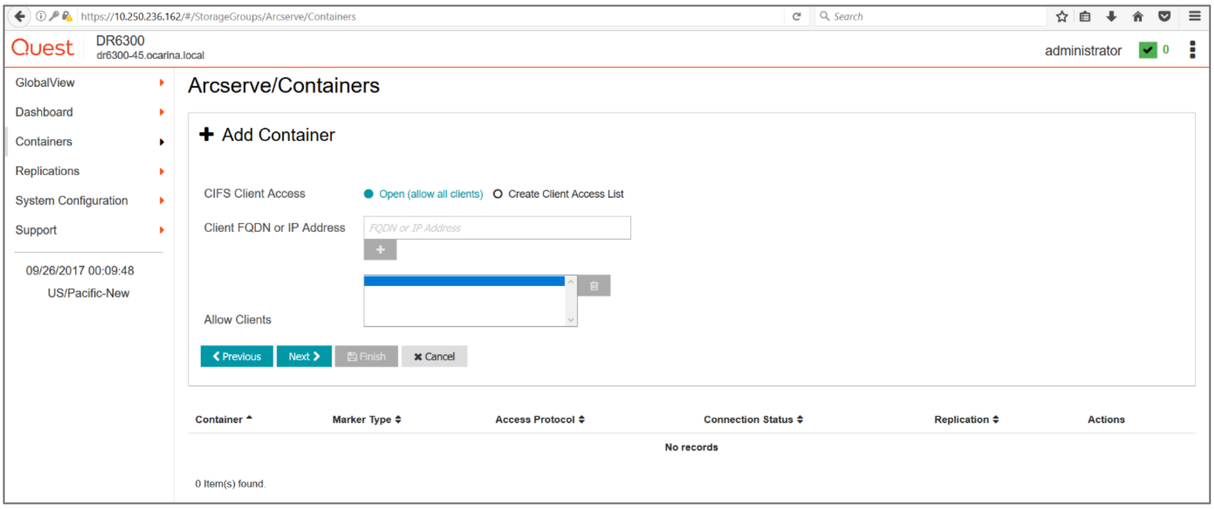
Client Access ● Open (allow all clients) ○ Create Client Access List

Client FQDN or IP Address FQDN or IP Address

Allow Clients

Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
No records					

0 Item(s) found.



Arcserve/Containers

Add Container

CIFS Client Access ● Open (allow all clients) ○ Create Client Access List

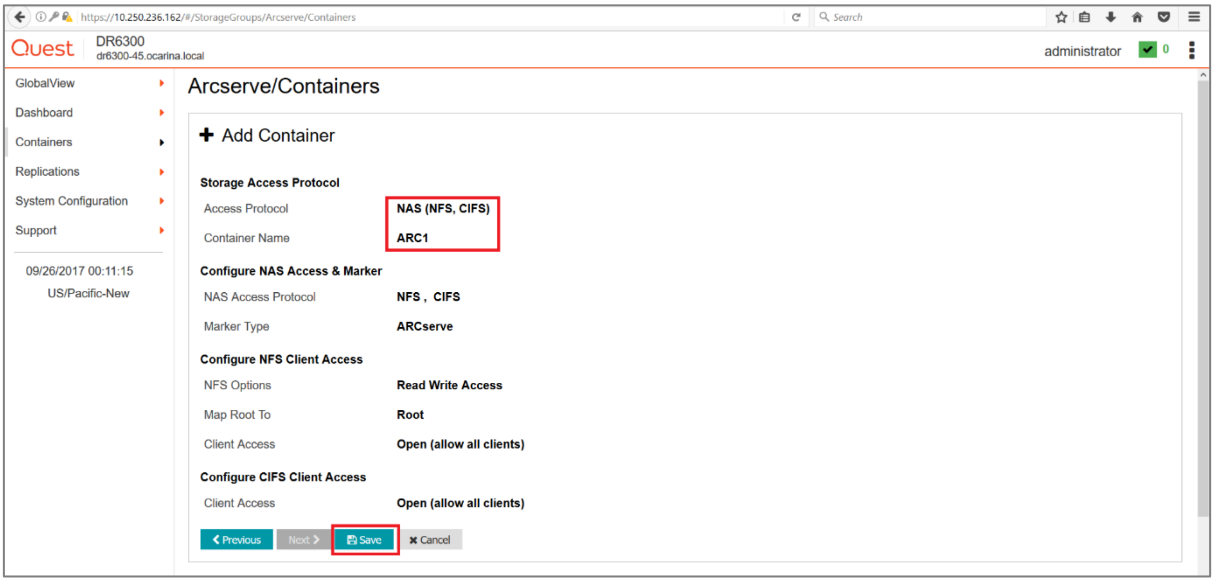
Client FQDN or IP Address FQDN or IP Address

Allow Clients

Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
No records					

0 Item(s) found.

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



Arcserve/Containers

+ Add Container

Storage Access Protocol

Access Protocol	**NAS (NFS, CIFS)**
Container Name	**ARC1**

Configure NAS Access & Marker

NAS Access Protocol	**NFS , CIFS**
Marker Type	**ARCserve**

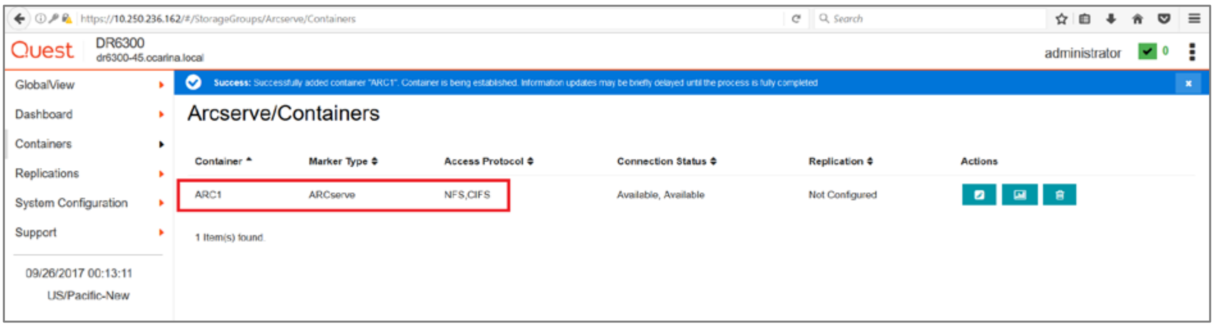
Configure NFS Client Access

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)**

16 Confirm that the container is added.



Success: Successfully added container "ARC1". Container is being established. Information updates may be briefly delayed until the process is fully completed

Arcserve/Containers

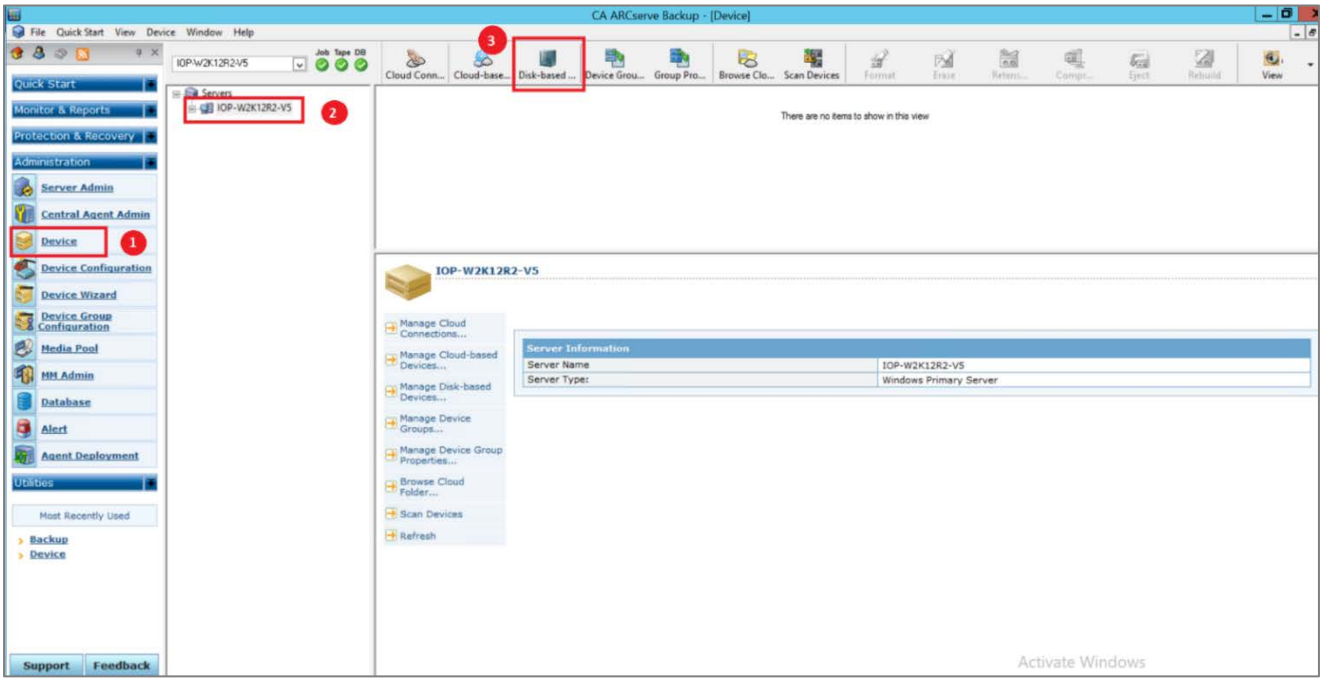
Container ▲	Marker Type ⬍	Access Protocol ⬍	Connection Status ⬍	Replication ⬍	Actions
ARC1	ARCserve	NFS,CIFS	Available, Available	Not Configured	

1 Item(s) found.

Creating a disk-based target device on CA ARCserve

For the Windows environment

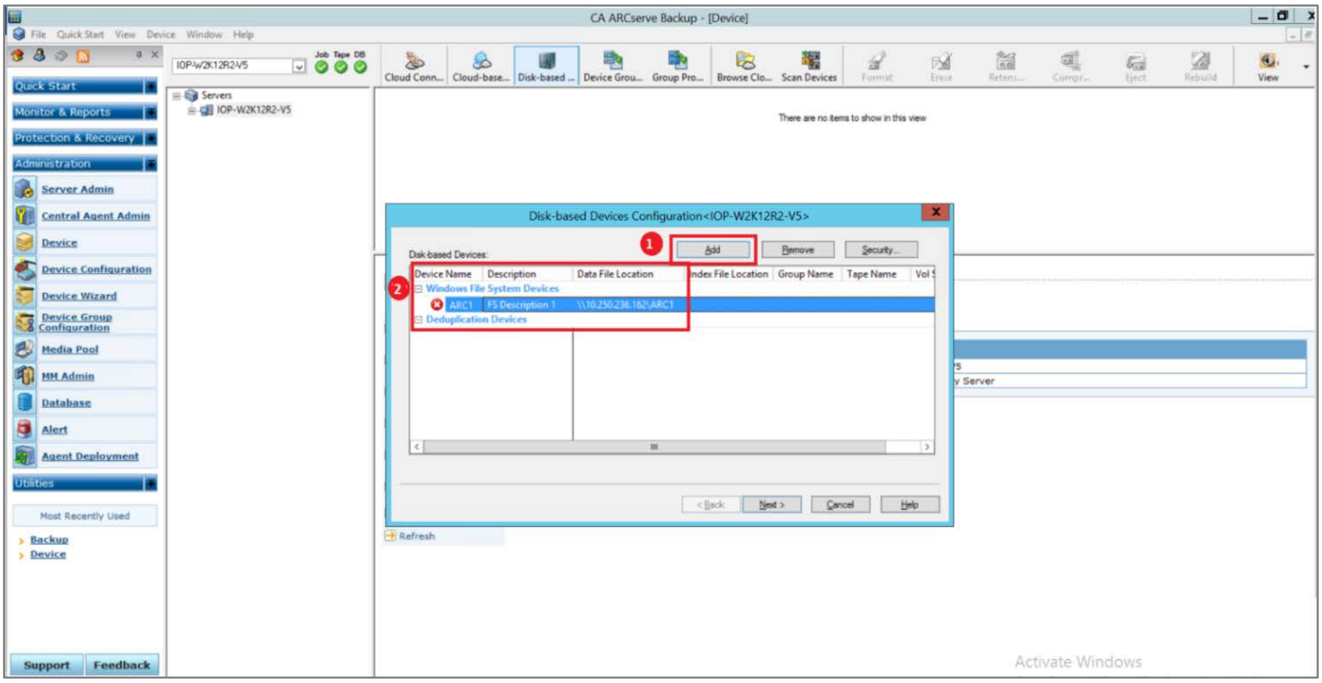
1. Open the **CA ARCserve Manager**. In the navigation pane, expand **Administration**, and click **Device**.
2. Select a server and click **Disk-Based Device**.



There are no items to show in this view

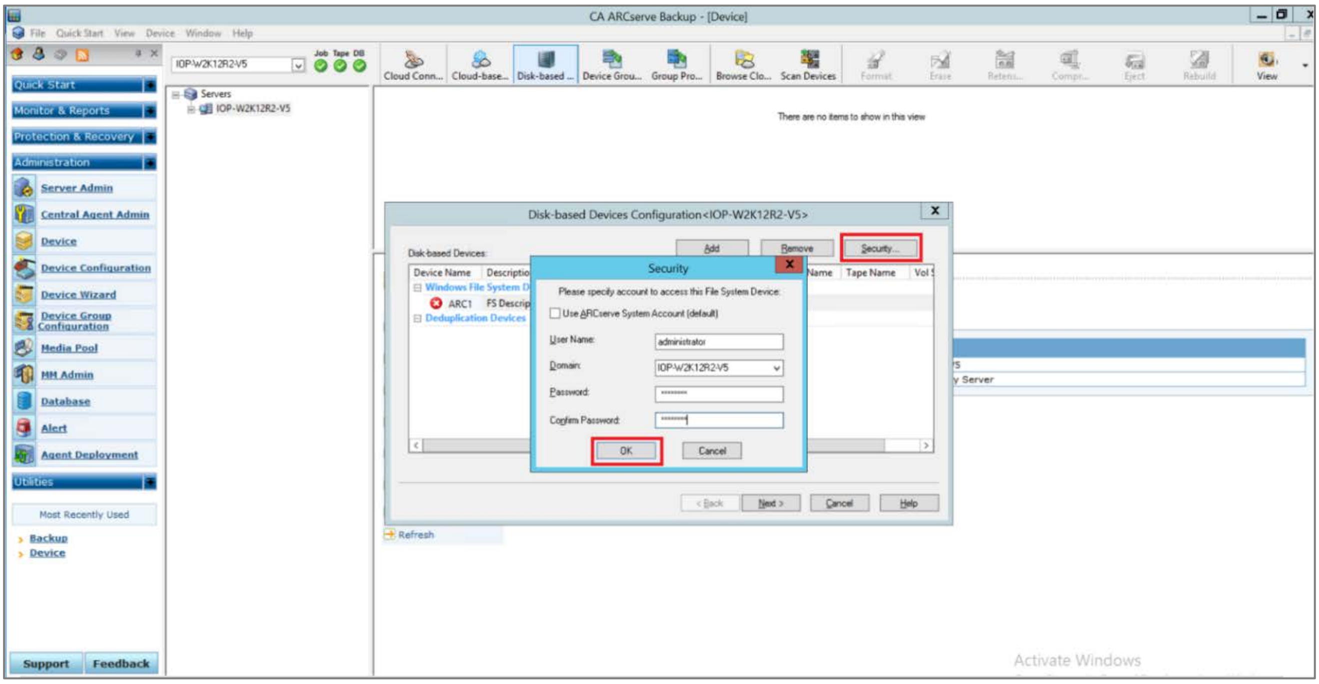
Server Information	
Server Name	IOP-W2K12R2-V5
Server Type:	Windows Primary Server

3. Select **Windows File System Devices** and enter a Device name, Description and the DR container share path as **Data File Location.**



Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vol
Windows File System Devices						
ARC1	FS Description 1	\\10.250.236.162\ARC1				
Deduplication Devices						

4 Click **Security**, and enter the credentials of the domain to access the share. Click **OK**.



Please specify account to access this File System Device:

☐ Use ARCserve System Account (default)

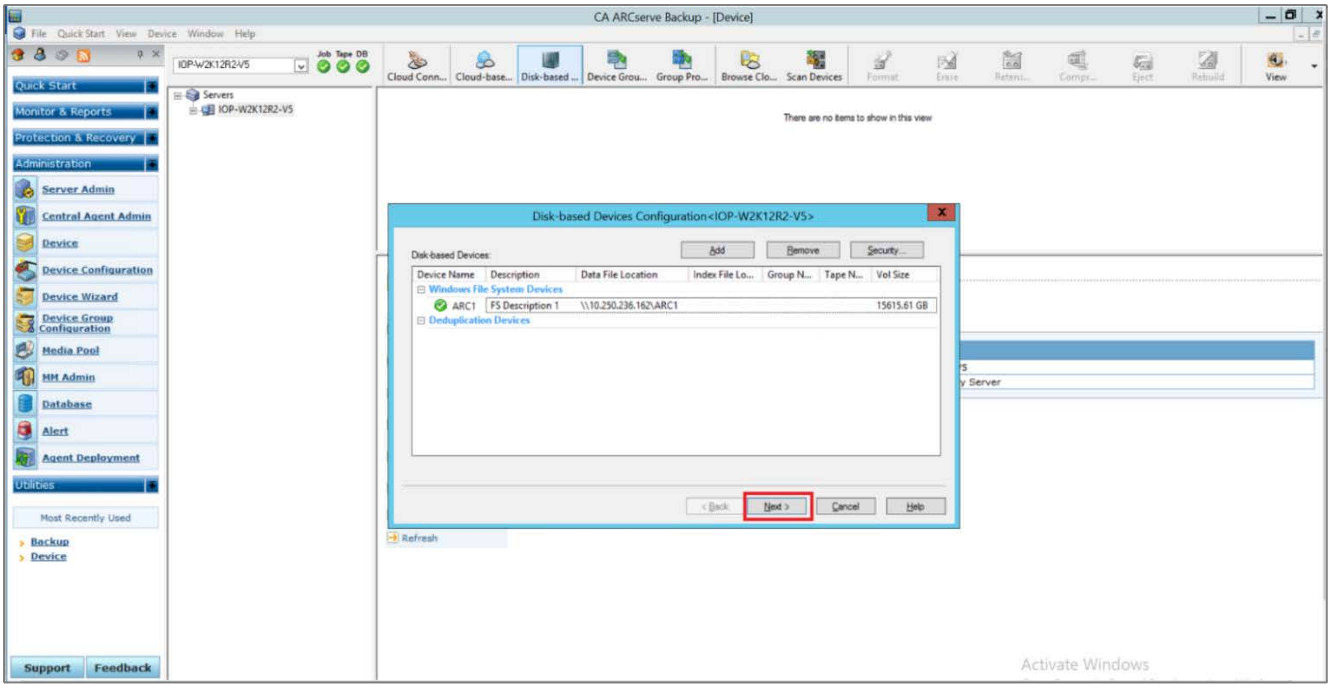
User Name: administrator

Domain: IOP-W2K12R2-V5

Password: ********

Confirm Password: ********

5 Click **Next** and then click **Finish**.



There are no items to show in this view

Disk-based Devices Configuration<IOP-W2K12R2-V5>

Disk-based Devices:

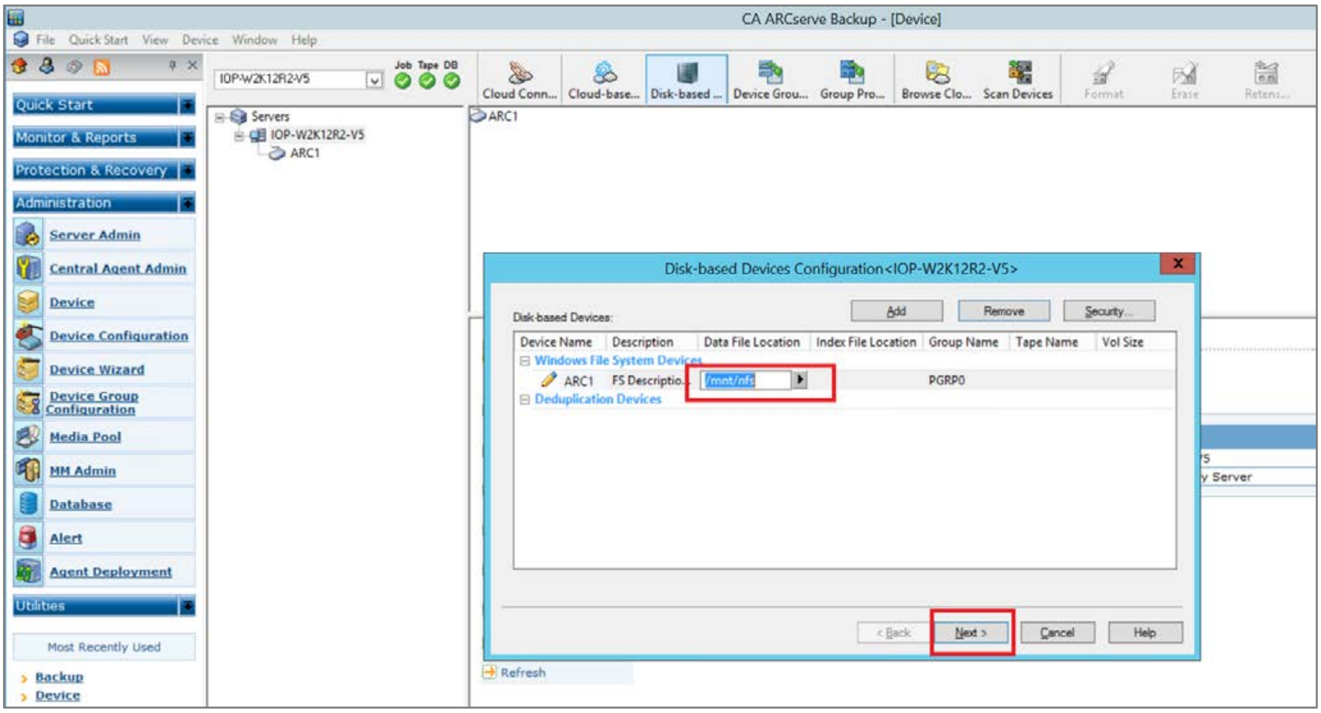
Device Name	Description	Data File Location	Index File Lo...	Group N...	Tape N...	Vol Size
Windows File System Devices						
ARC1	FS Description 1	\\10.250.236.162\ARC1				15615.61 GB
Deduplication Devices						

NOTE: Make sure that you can mount/verify the NFS share from the UNIX/Linux client system. Please see **Appendix A.1** for how to mount/verify the NFS share.

For the Unix/Linux environment

The steps described below for the Unix/Linux environment are similar to the procedure for the Windows environment. The only difference is that the DR Series container NFS export path is used instead of a UNC path, as described below, for **Data File Location**.

For other details, please refer to the preceding section for the Windows Environment.


CA ARCserve Backup - [Device]

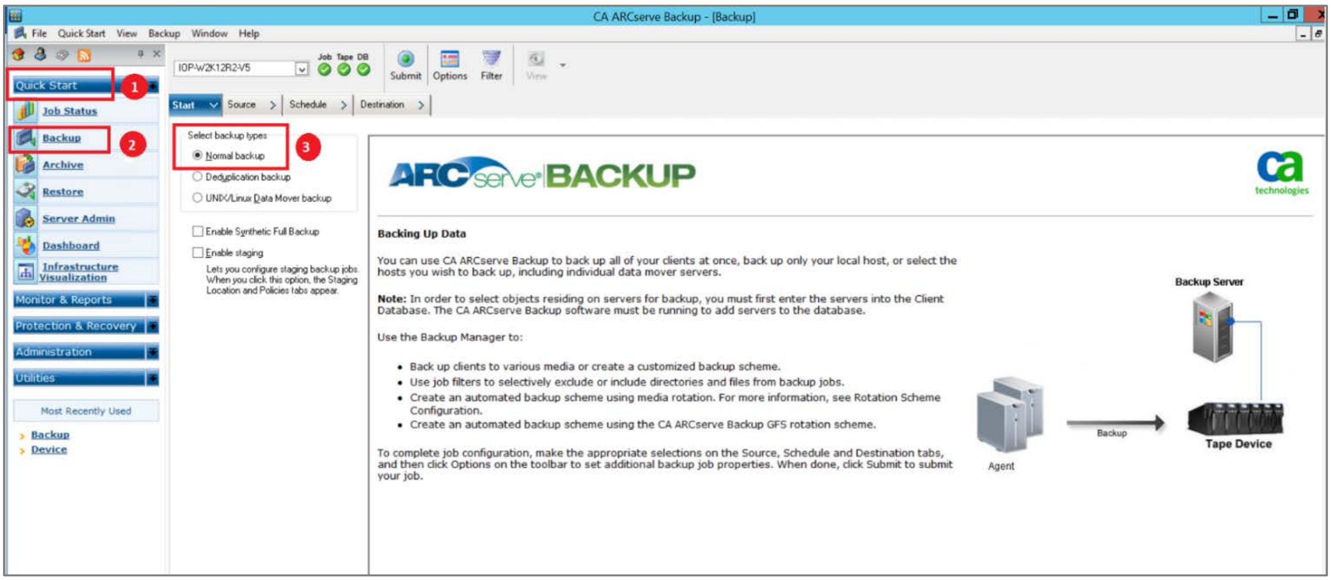
Disk-based Devices Configuration<IOP-W2K12R2-V5>

Disk-based Devices:

Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vol Size
Windows File System Devices						
ARC1	FS Descriptio...	/mnt/nfs		PGRP0		
Deduplication Devices						

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

1 In the Navigation pane, click **Quick start -> Backup**. Then, in the right side panel, on the **Start** tab, set Select backup types as **Normal backup** for both CIFS and NFS backup.



Select backup types

● Normal backup

○ Deduplication backup

○ UNIX/Linux Data Mover backup

□ Enable Synthetic Full Backup

□ Enable staging

Lets you configure staging backup jobs. When you click this option, the Staging Location and Policies tabs appear.

Backing Up Data

You can use CA ARCserve Backup to back up all of your clients at once, back up only your local host, or select the hosts you wish to back up, including individual data mover servers.

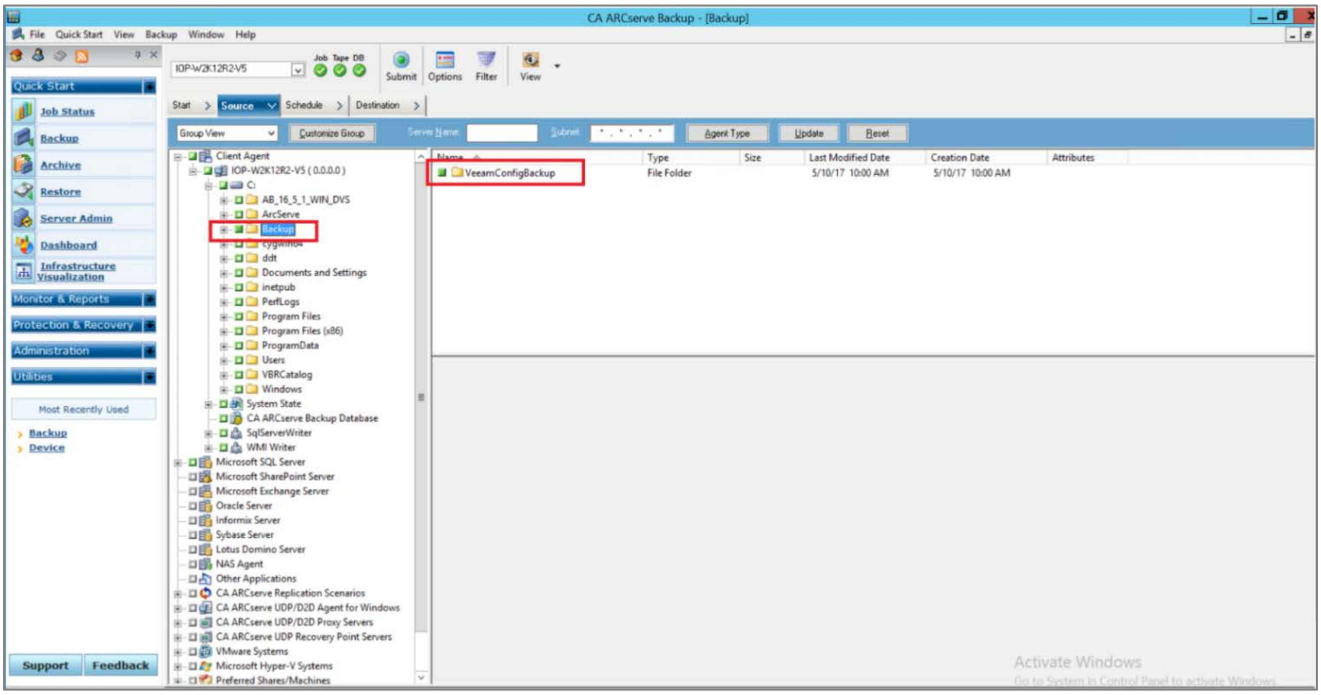
Note: In order to select objects residing on servers for backup, you must first enter the servers into the Client Database. The CA ARCserve Backup software must be running to add servers to the database.

Use the Backup Manager to:

- Back up clients to various media or create a customized backup scheme.
- Use job filters to selectively exclude or include directories and files from backup jobs.
- Create an automated backup scheme using media rotation. For more information, see Rotation Scheme Configuration.
- Create an automated backup scheme using the CA ARCserve Backup GFS rotation scheme.

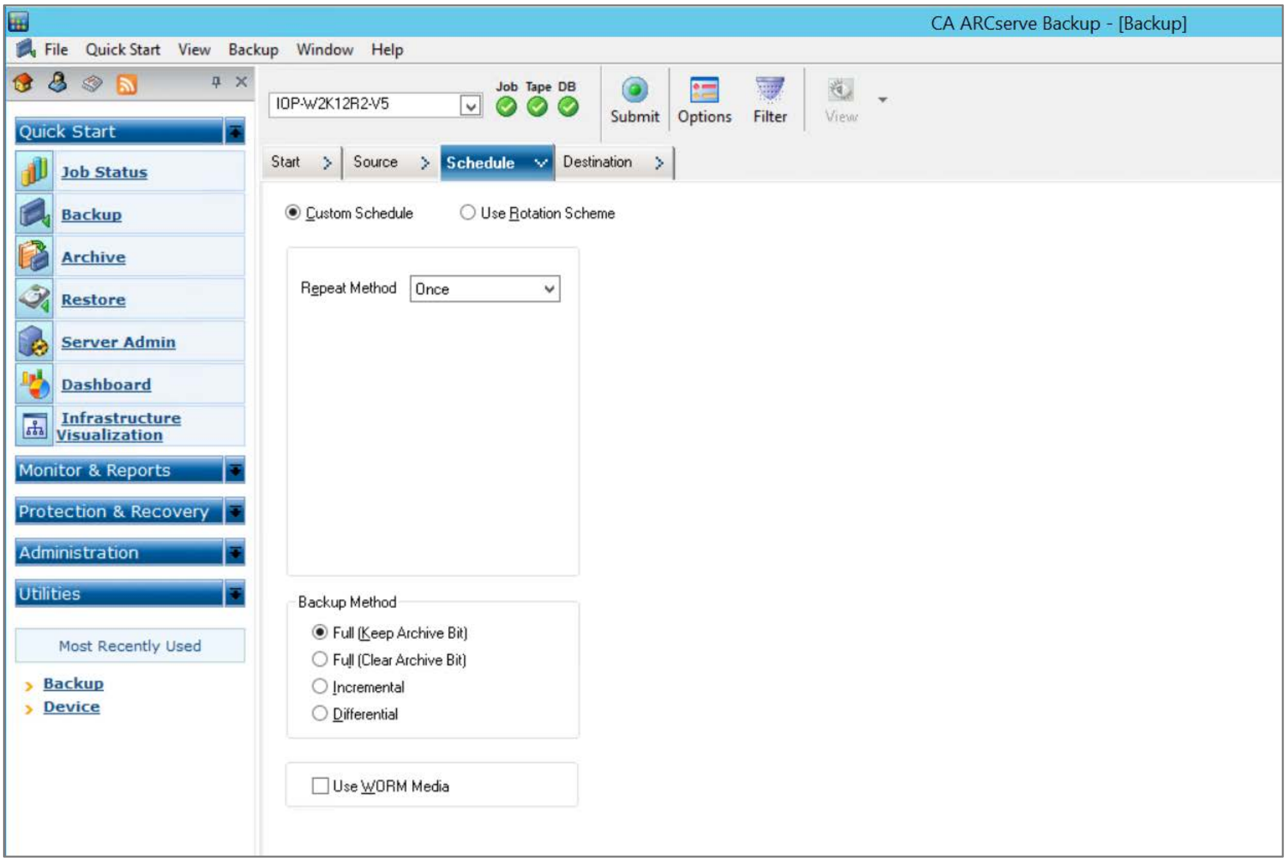
To complete job configuration, make the appropriate selections on the Source, Schedule and Destination tabs, and then click Options on the toolbar to set additional backup job properties. When done, click Submit to submit your job.

2 On the **Source** tab, select the backup source files.



Name	Type	Size	Last Modified Date	Creation Date	Attributes
VeeamConfigBackup	File Folder		5/10/17 10:00 AM	5/10/17 10:00 AM	

3 On **Schedule** tab, set a **Custom Schedule** or Use **Rotation Schema** and Backup Method.



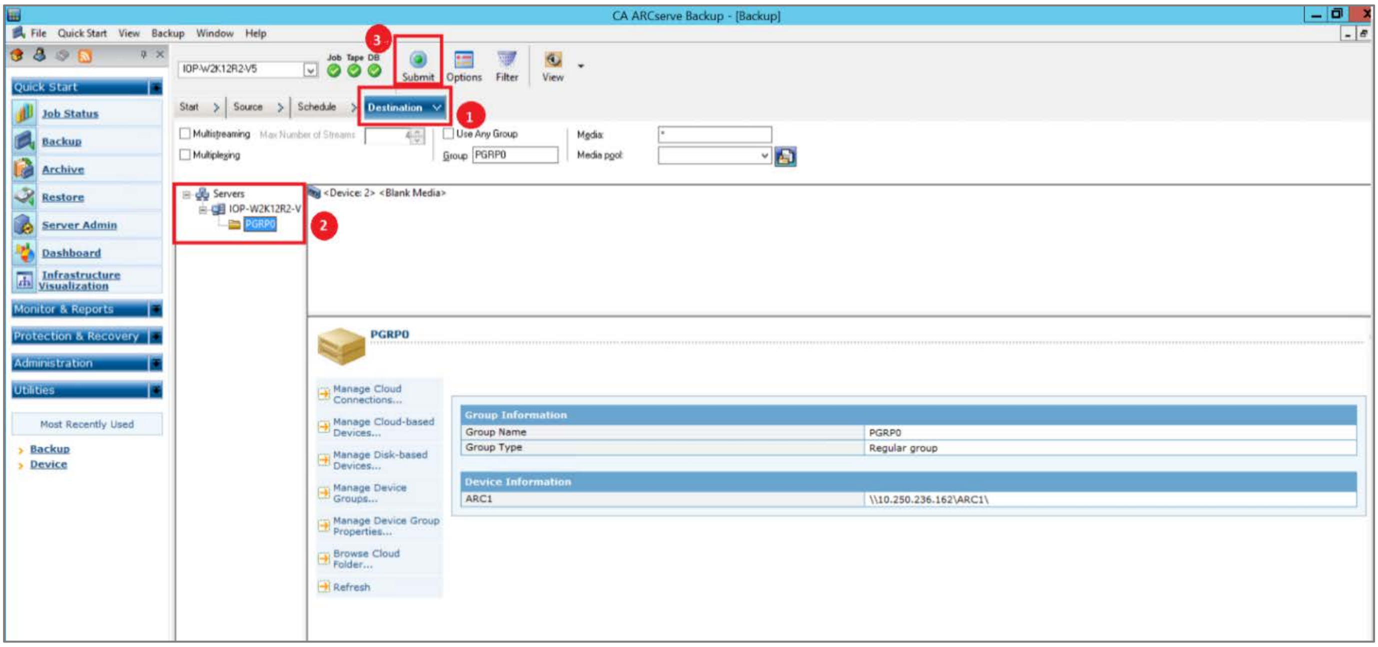
● Custom Schedule ○ Use Rotation Scheme

Repeat Method: Once

Backup Method
- ● Full (Keep Archive Bit)
- ○ Full (Clear Archive Bit)
- ○ Incremental
- ○ Differential

□ Use WORM Media

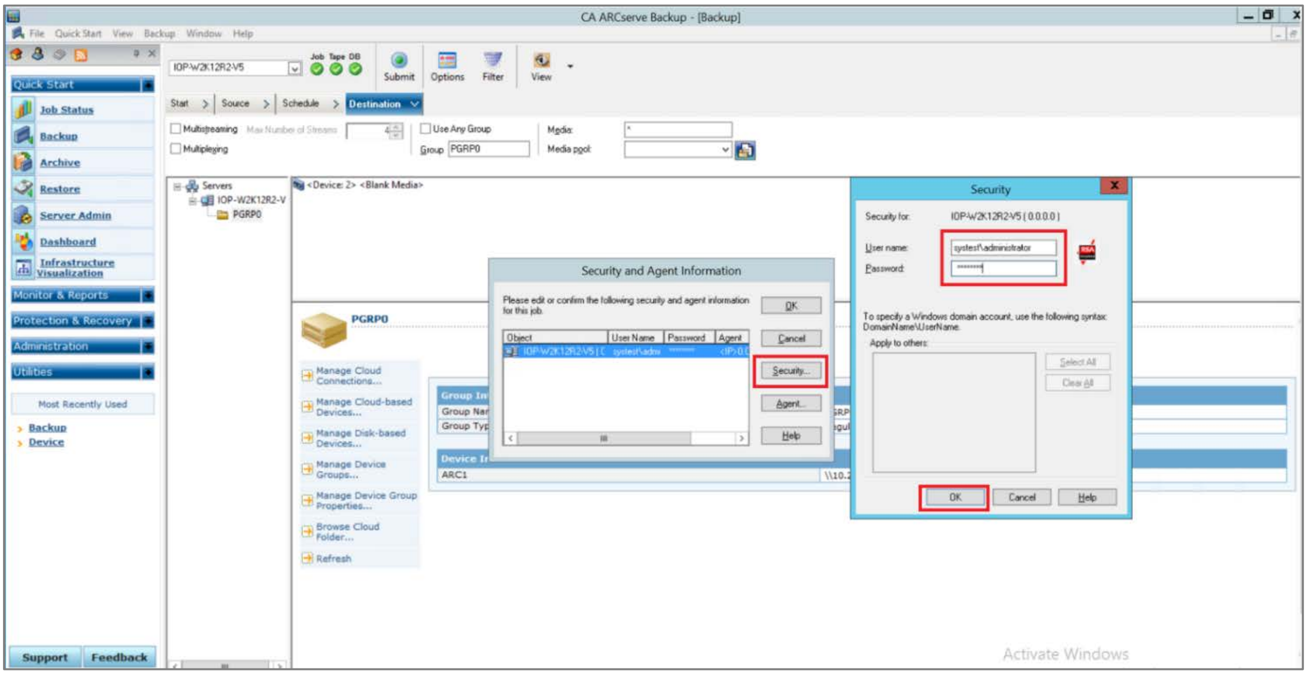
4 On the **Destination** tab, select a destination device that is created on the DR Series system, and click **Submit**.



Group Information	
Group Name	PGRP0
Group Type	Regular group

Device Information	
ARC1	\\10.250.236.162\ARC1\

5 In the **Security and Agent Information** window, choose an agent server, click **Security**, and, in the Security window, enter a password and click **OK**.



Please edit or confirm the following security and agent information for this job.

IOP-W2K12R2-V5 | C: systest\adm ******

Security for: IOP-W2K12R2-V5 (0.0.0.0)

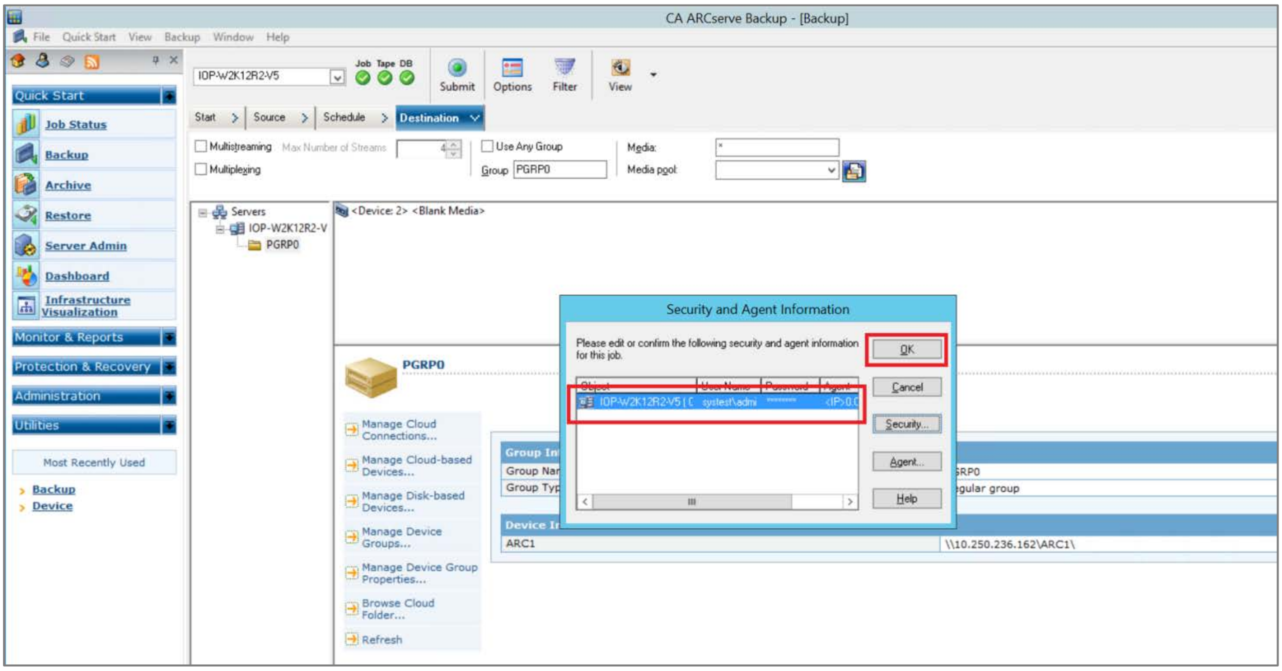
User name: systest\administrator

Password: ********

To specify a Windows domain account, use the following syntax: DomainName\UserName.

Apply to others:

6 Click **OK** in the Security and Agent Information Window.



IOP-W2K12R2-V5

□ Multistreaming Max Number of Streams

□ Multiplexing

□ Use Any Group

Group: PGRP0

Media: *

Media pool:

<Device: 2> <Blank Media>

Security and Agent Information

Please edit or confirm the following security and agent information for this job.

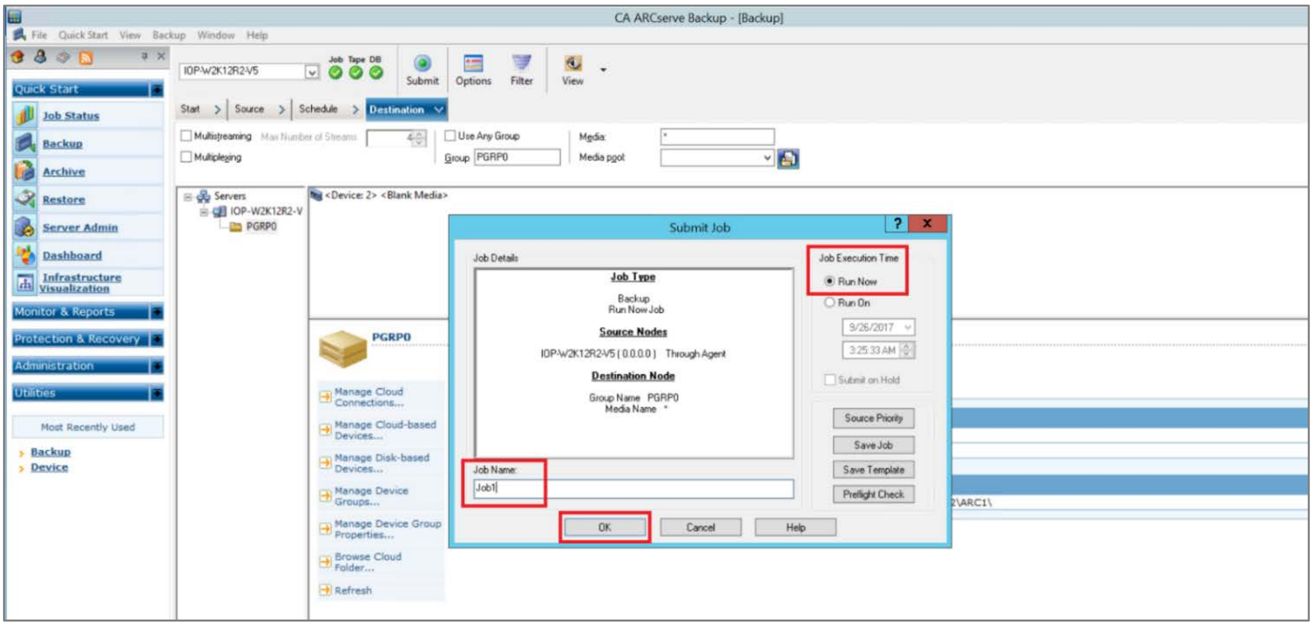
Object	User Name	Password	Agent
IOP-W2K12R2-V5 (C	systest\admi	********	<IP>0.0

Group Name: PGRP0

Group Type: Regular group

Device Name: ARC1 \\10.250.236.162\ARC1\

7 Enter the **backup Job Name**, choose a **Job Execution Time**, and then click **OK**.



Submit Job

Job Details

Job Type

Backup
Run Now Job

Source Nodes

IOP-W2K12R2-V5 (0.0.0.0) Through Agent

Destination Node

Group Name PGRP0
Media Name *

Job Name: Job1

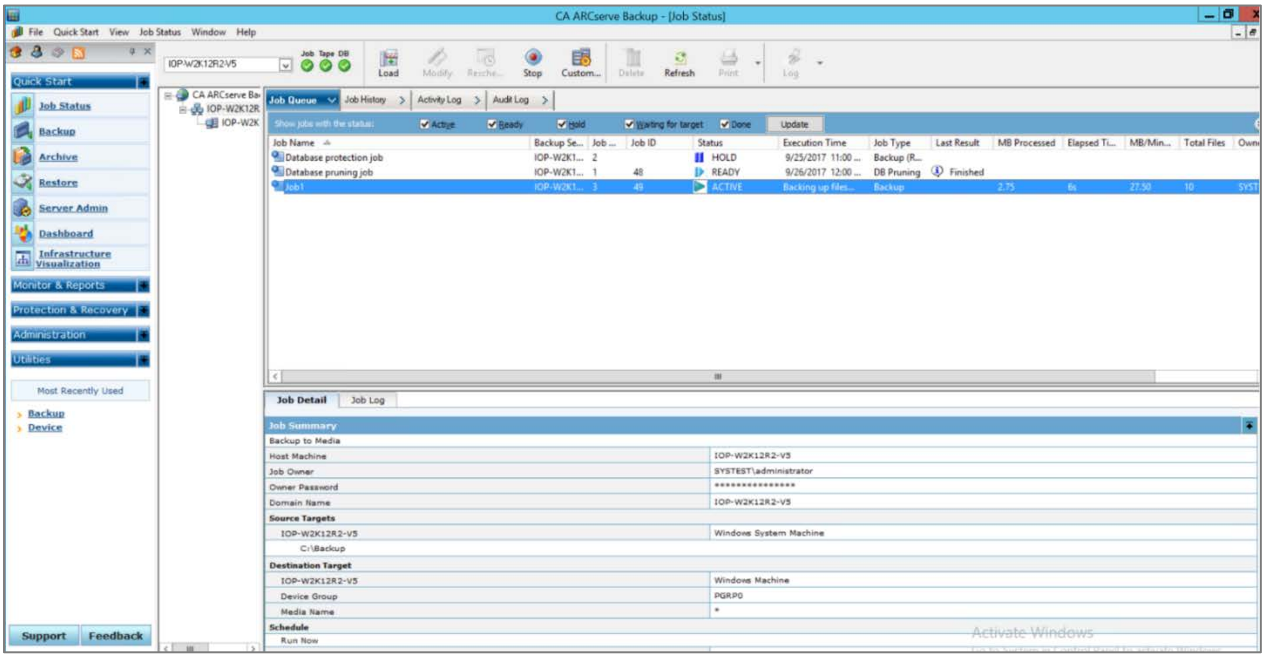
Job Execution Time

● Run Now

○ Run On 9/26/2017 3:25:33 AM

□ Submit on Hold

8 When the backup job runs, check the Job Queue display in **Job Status** window.



Job Name	Backup Se...	Job ...	Job ID	Status	Execution Time	Job Type	Last Result	MB Processed	Elapsed Ti...	MB/Min...	Total Files	Own
Database protection job	IOP-W2K1...	2		HOLD	9/25/2017 11:00 ...	Backup (R...						
Database pruning job	IOP-W2K1...	1	48	READY	9/26/2017 12:00 ...	DB Pruning	Finished					
Job1	IOP-W2K1...	3	49	ACTIVE	Backing up files...	Backup		2.75	6s	27.50	10	SYST

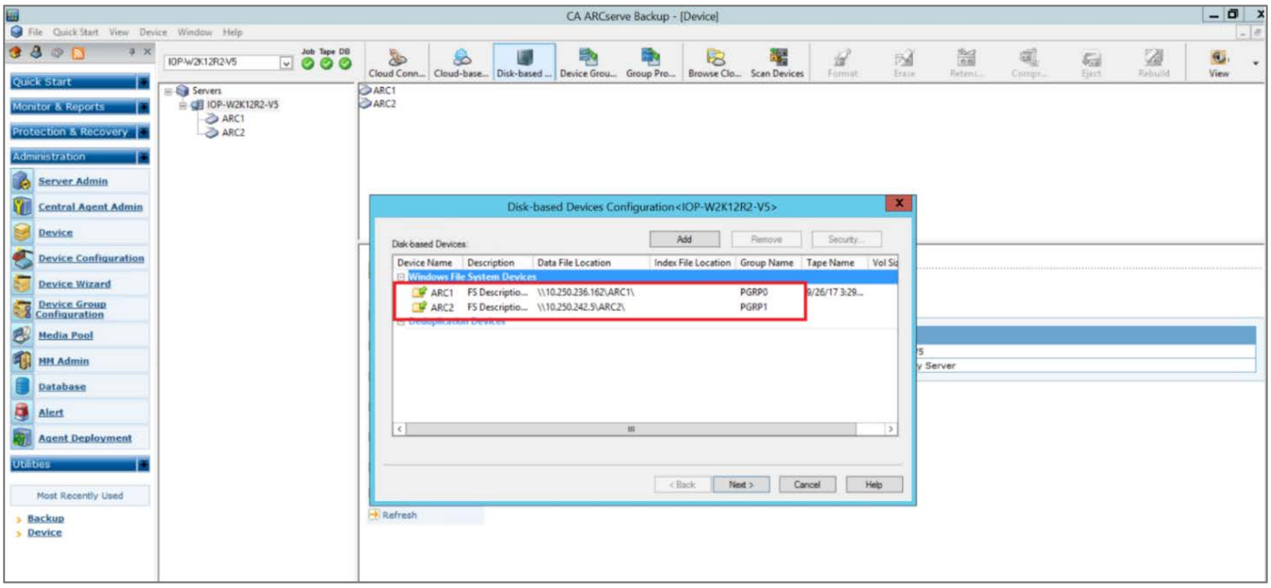
Job Summary	
Backup to Media	
Host Machine	IOP-W2K12R2-V5
Job Owner	SYSTEST\administrator
Owner Password	***************
Domain Name	IOP-W2K12R2-V5
Source Targets	
IOP-W2K12R2-V5	Windows System Machine
C:\Backup	
Destination Target	
IOP-W2K12R2-V5	Windows Machine
Device Group	PGRP0
Media Name	*
Schedule	
Run Now	

4

Setting up DR native replication & restoring from a replication target

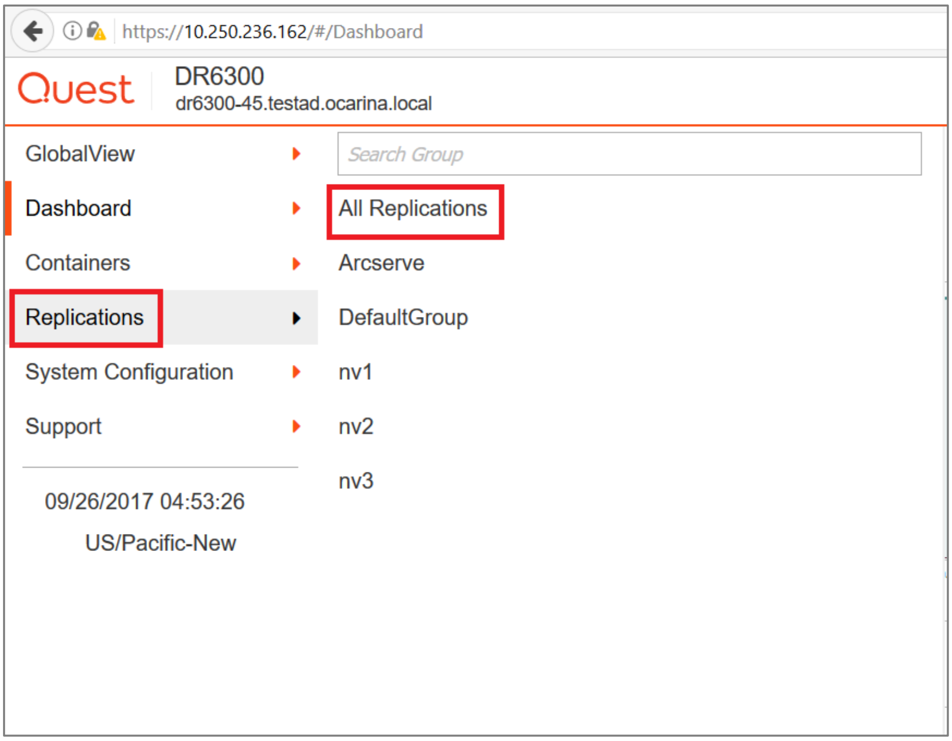
Creating a DR Series replication session

1 Create a CIFS container **'ARC1'** on DR1; create a second CIFS container **'ARC2'** on DR2. For each of the containers, on the ARCServe server, configure a Windows File System Device within the same group.

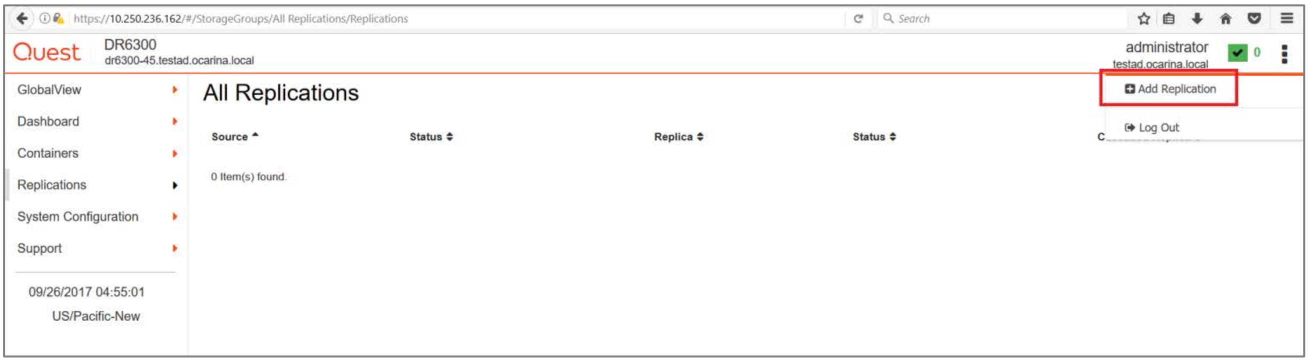


Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vol Siz
Windows File System Devices						
ARC1	FS Descriptio...	\\10.250.236.162\ARC1\		PGRP0	9/26/17 3:29...	
ARC2	FS Descriptio...	\\10.250.242.5\ARC2\		PGRP1		
Deduplication Devices						

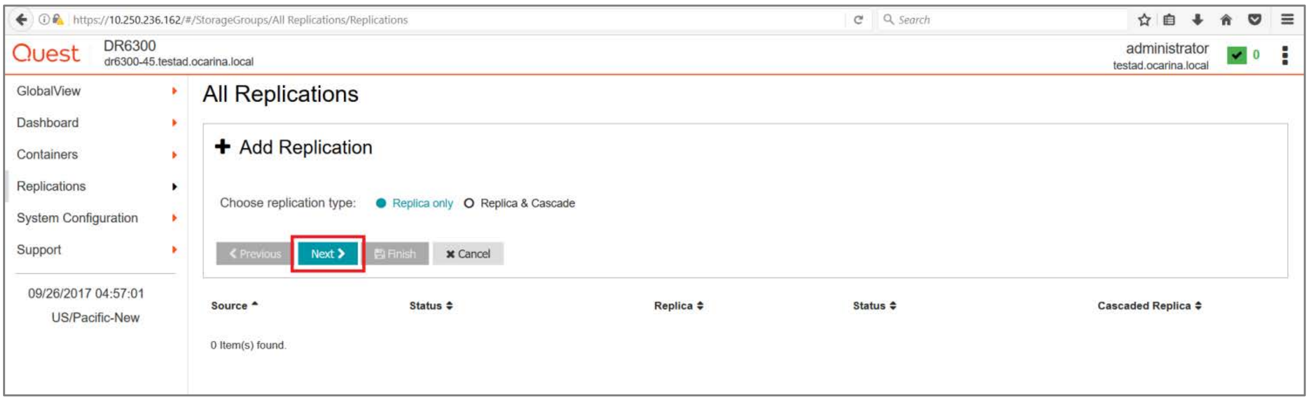
2 On the source DR Series system, click **Replication** in the left navigation menu, and then click **All Replications**.



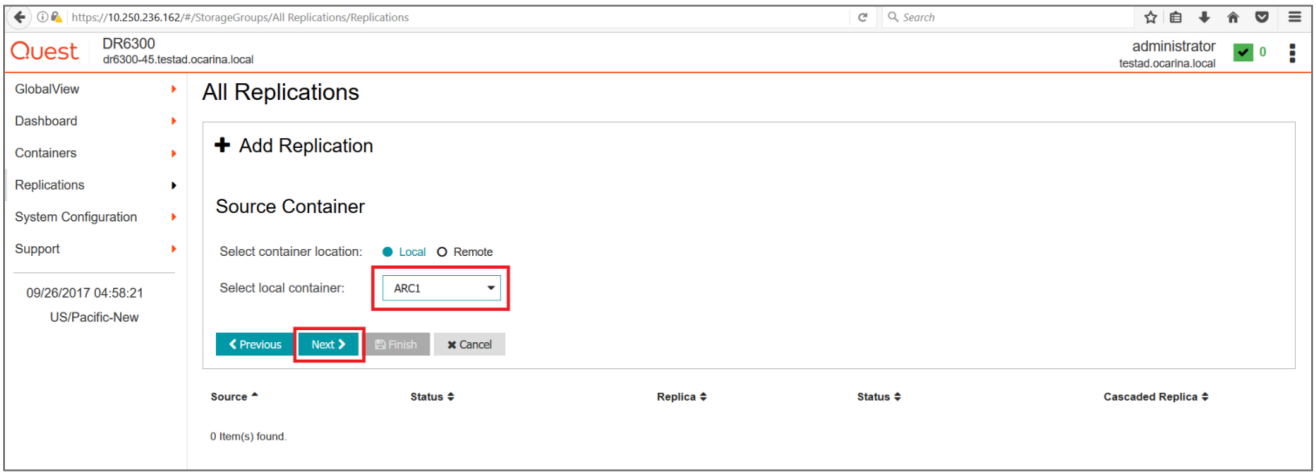
3 Select **Add Replication** from the Action Menu.



4 Under **All Replications**, select the required Replication type and click **Next.**



5 In the **Add Replication dialog** box, select the container from the Local System drop down menu, and then select the **'ARC1'** container.



https://10.250.236.162/#/StorageGroups/All Replications/Replications

Quest DR6300
dr6300-45.testad.ocarina.local

administrator
testad.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

09/26/2017 04:58:21
US/Pacific-New

All Replications

Add Replication

Source Container

Select container location: ● Local ○ Remote

Select local container: ARC1

Previous | Next | Finish | Cancel

Source	Status	Replica	Status	Cascaded Replica

0 Item(s) found.

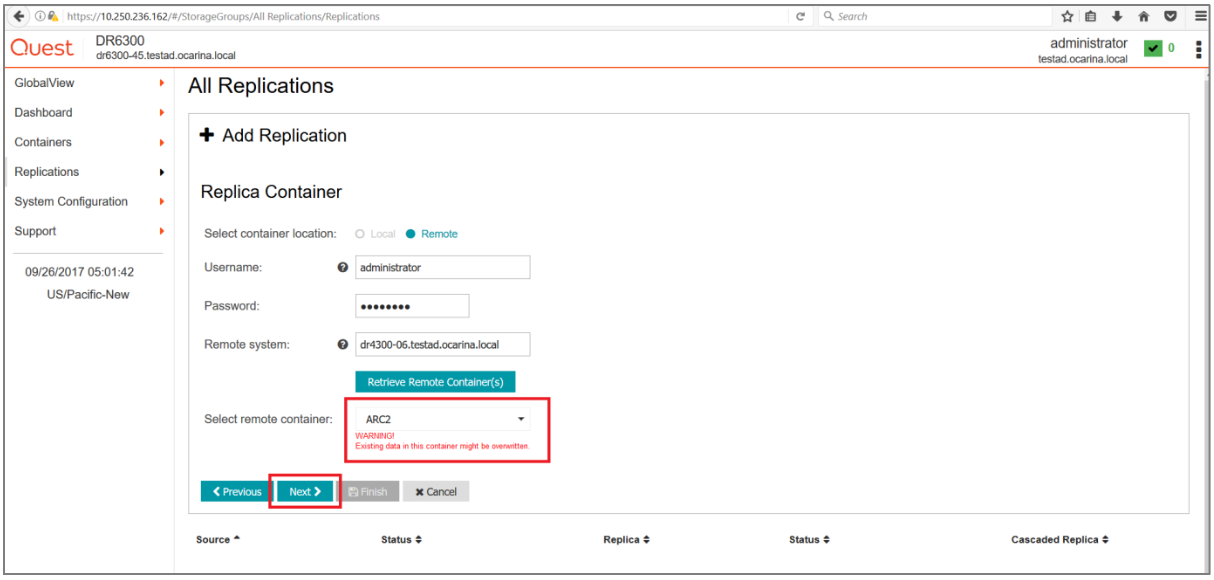
6 Configure the Replica Container as follows:

a Select the option, Select container from **Remote** system

b Enter the target DR Series system login credentials.

c Click **Retrieve Remote Containers**, and then select the **‘ARC2’** container from the list.

d Click **Next** and then **Finish**.



https://10.250.236.162/#/StorageGroups/All Replications/Replications

Quest DR6300
dr6300-45.testad.ocarina.local

administrator
testad.ocarina.local

GlobalView
Dashboard
Containers
Replications
System Configuration
Support

09/26/2017 05:01:42
US/Pacific-New

All Replications

Add Replication

Replica Container

Select container location: ○ Local ● Remote

Username: administrator

Password: ••••••••

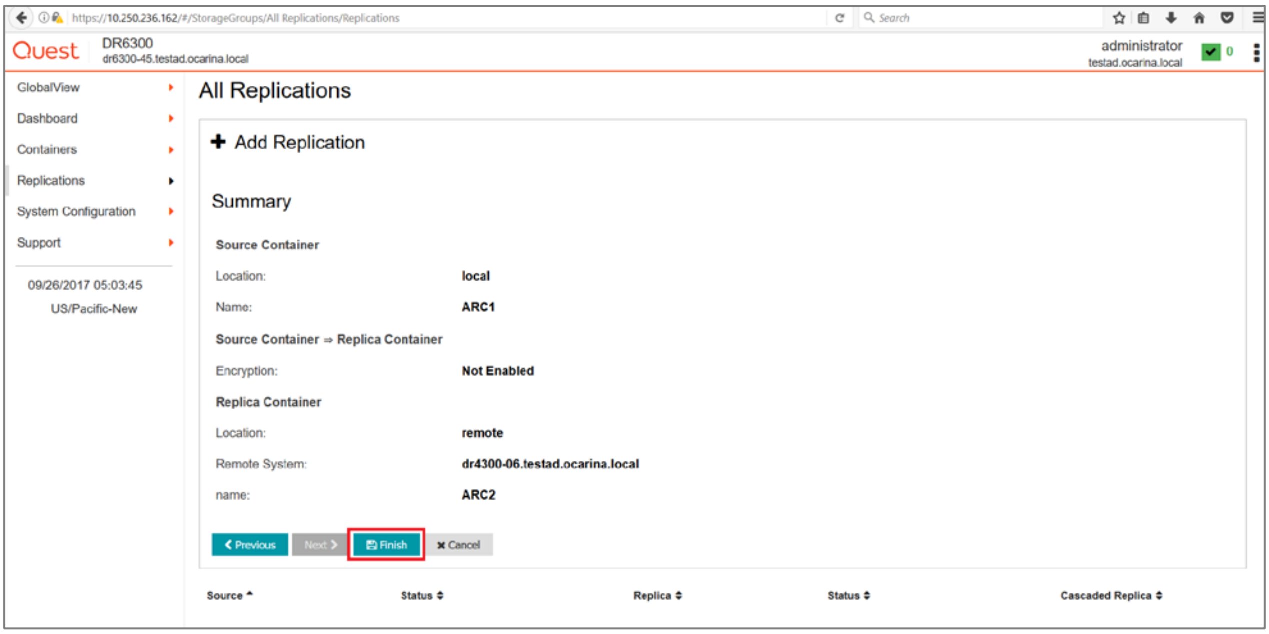
Remote system: dr4300-06.testad.ocarina.local

Retrieve Remote Container(s)

Select remote container: ARC2
WARNING!
Existing data in this container might be overwritten.

Previous | Next | Finish | Cancel

Source	Status	Replica	Status	Cascaded Replica



All Replications

✚ Add Replication

Summary

Source Container

Location: **local**

Name: **ARC1**

Source Container ⇒ Replica Container

Encryption: **Not Enabled**

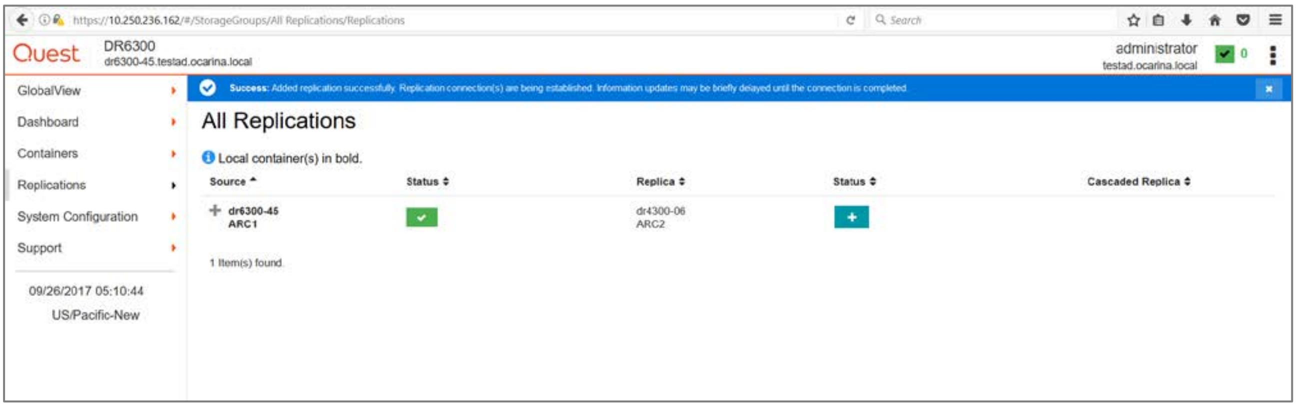
Replica Container

Location: **remote**

Remote System: **dr4300-06.testad.ocarina.local**

name: **ARC2**

7 Verify that the replication is created successfully, and that the Status column shows a check box for the replication session.



Success: Added replication successfully. Replication connection(s) are being established. Information updates may be briefly delayed until the connection is completed.

All Replications

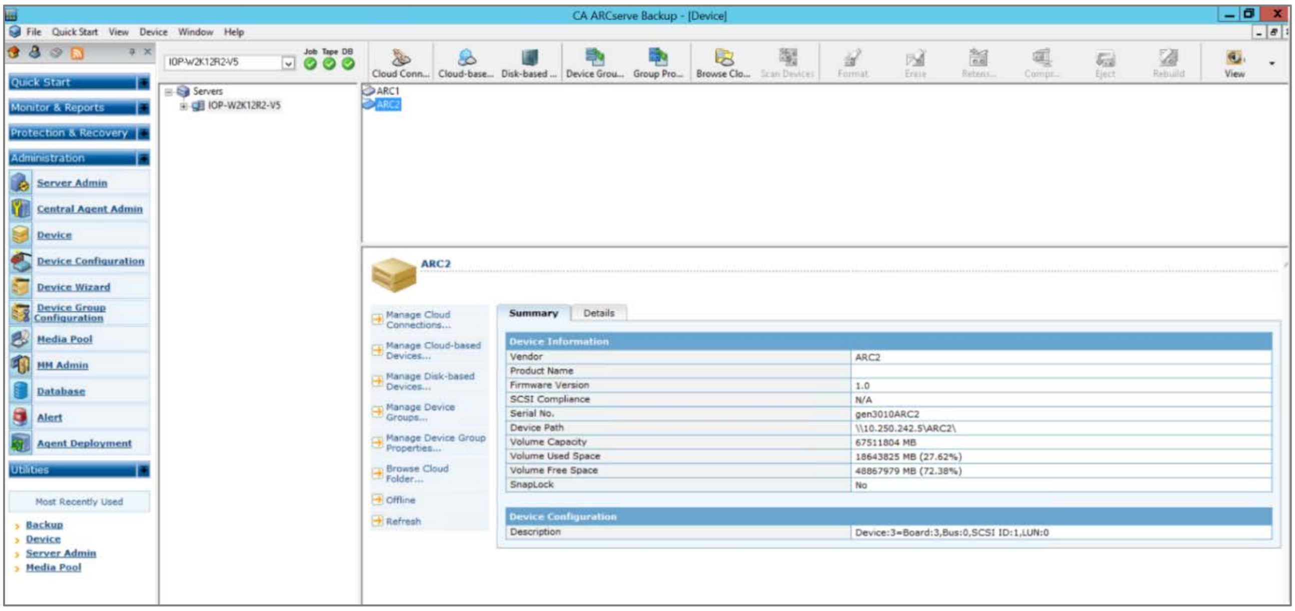
Local container(s) in bold.

Source	Status	Replica	Status	Cascaded Replica
dr6300-45 **ARC1**	✓	dr4300-06 ARC2	+	

1 Item(s) found.

Restoring from the replication target

1 Restart the ARCserve services, navigate to **Administration > Device**, and then verify the target device.



CA ARCserve Backup - [Device]
File Quick Start View Device Window Help
Quick Start
Monitor & Reports
Protection & Recovery
Administration
Server Admin
Central Agent Admin
Device
Device Configuration
Device Wizard
Device Group Configuration
Media Pool
MM Admin
Database
Alert
Agent Deployment
Utilities
Most Recently Used
Backup
Device
Server Admin
Media Pool
IOP-W2K12R2-V5
Job Tape DB
Servers
IOP-W2K12R2-V5
ARC1
ARC2
Cloud Conn... Cloud-base... Disk-based ... Device Grou... Group Pro... Browse Clo... Scan Devices Format Erase Retens... Compr... Eject Rebuild View
Manage Cloud Connections...
Manage Cloud-based Devices...
Manage Disk-based Devices...
Manage Device Groups...
Manage Device Group Properties...
Browse Cloud Folder...
Offline
Refresh

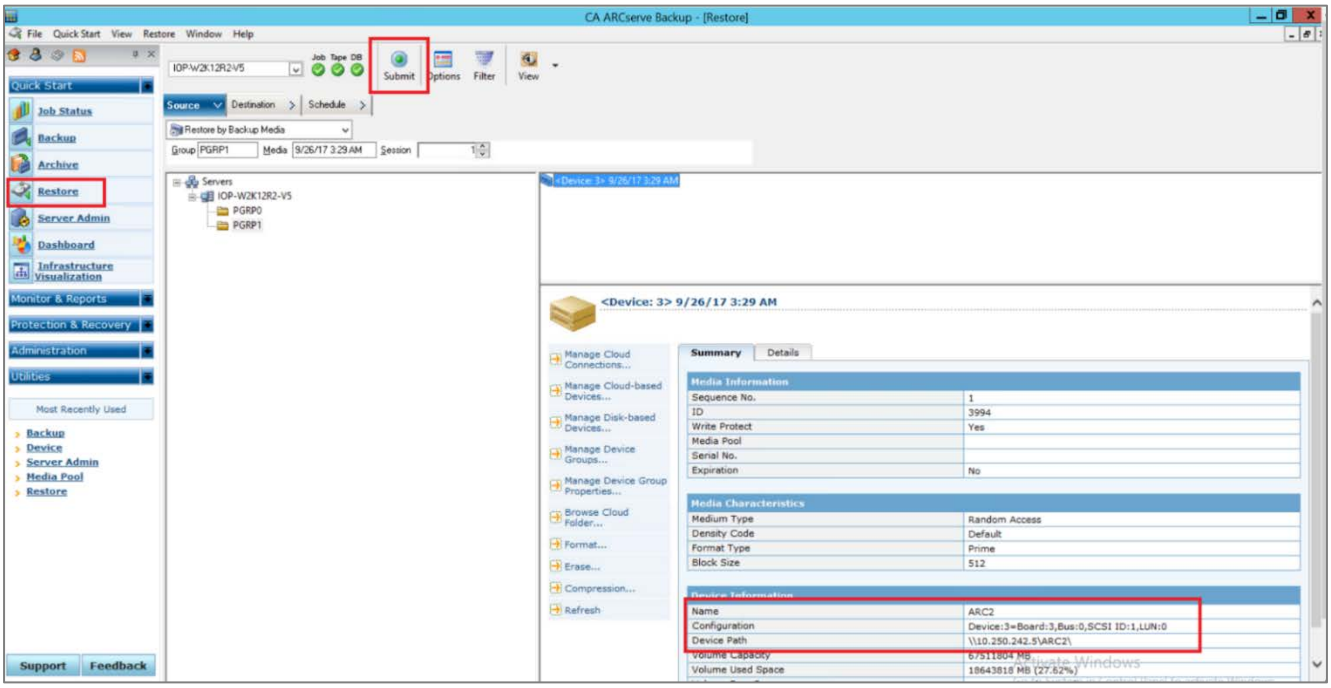
ARC2

Summary | Details

Device Information	
Vendor	ARC2
Product Name	
Firmware Version	1.0
SCSI Compliance	N/A
Serial No.	gen3010ARC2
Device Path	\\10.250.242.5\ARC2\
Volume Capacity	67511804 MB
Volume Used Space	18643825 MB (27.62%)
Volume Free Space	48867979 MB (72.38%)
SnapLock	No

Device Configuration	
Description	Device:3=Board:3,Bus:0,SCSI ID:1,LUN:0

2 Go to Quick Start > Restore, select Restore by Backup Media, and select the device.



Restore by Backup Media

Group: PGRP1 Media: 9/26/17 3:29 AM Session: 1

<Device: 3> 9/26/17 3:29 AM

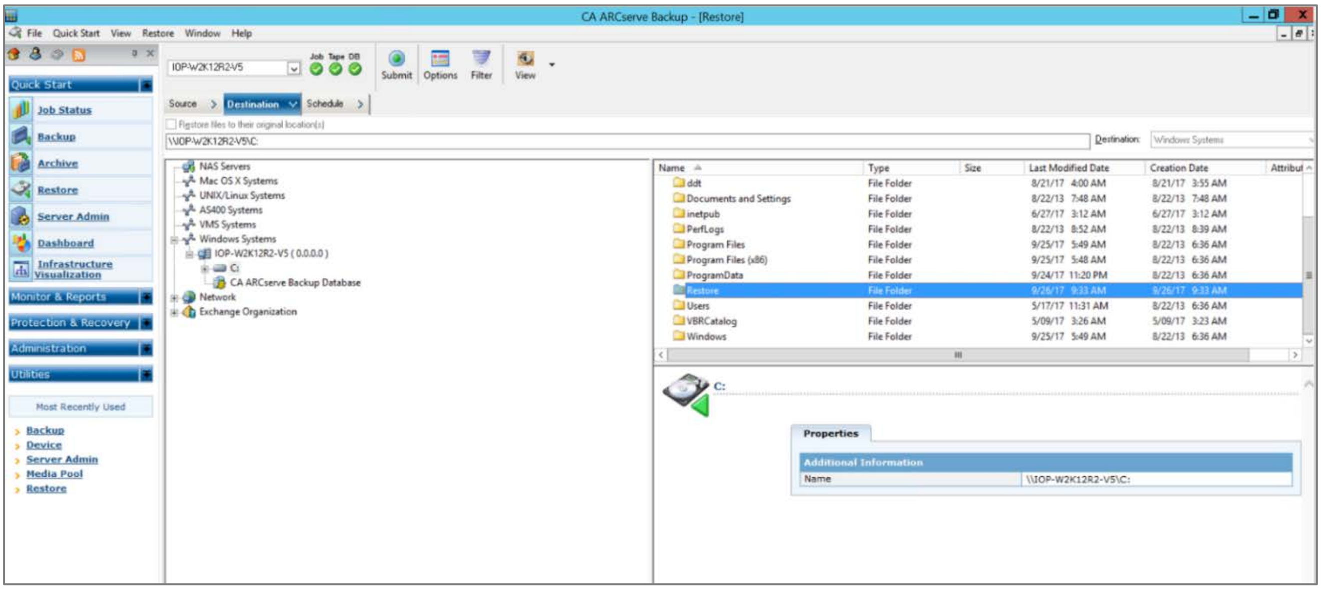
Summary | Details

Media Information	
Sequence No.	1
ID	3994
Write Protect	Yes
Media Pool	
Serial No.	
Expiration	No

Media Characteristics	
Medium Type	Random Access
Density Code	Default
Format Type	Prime
Block Size	512

Device Information	
Name	ARC2
Configuration	Device:3=Board:3,Bus:0,SCSI ID:1,LUN:0
Device Path	\\10.250.242.5\ARC2\
Volume Capacity	67511804 MB
Volume Used Space	18643818 MB (27.62%)

3 On the **Destination** tab, select the folder in which the Restore should take place.



IOP-W2K12R2-V5

□ Restore files to their original location(s)

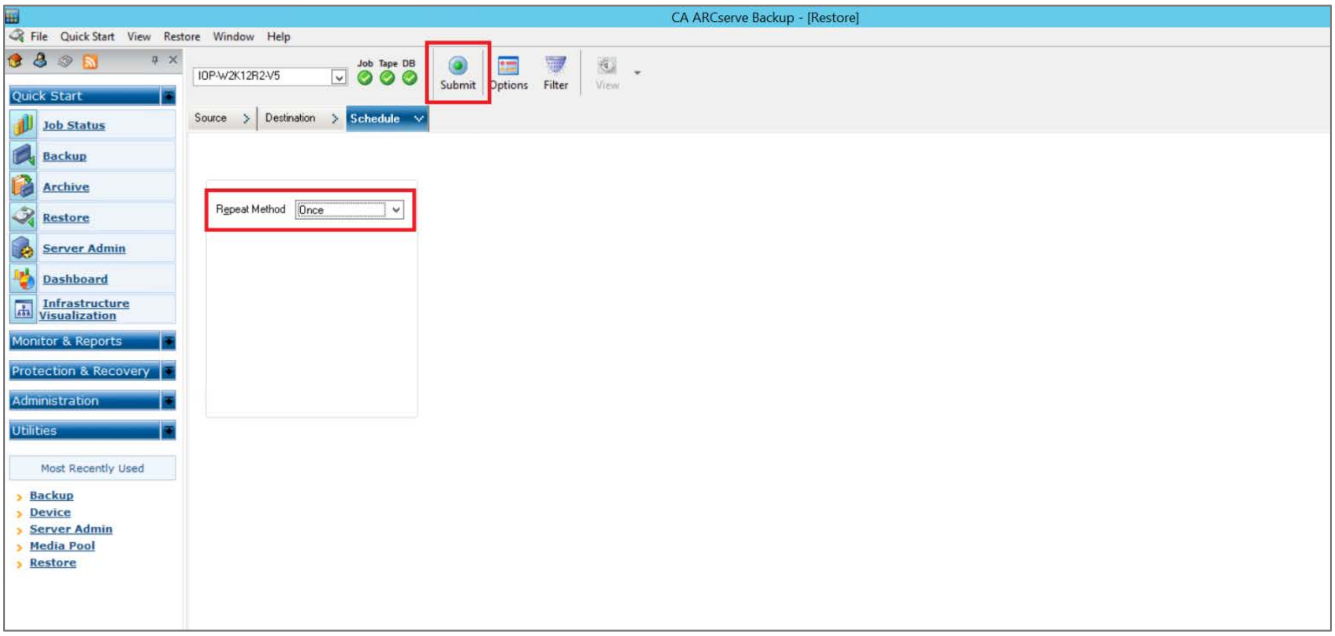
\\IOP-W2K12R2-V5\C:

Destination: Windows Systems

Name	Type	Size	Last Modified Date	Creation Date	Attribut
ddt	File Folder		8/21/17 4:00 AM	8/21/17 3:55 AM	
Documents and Settings	File Folder		8/22/13 7:48 AM	8/22/13 7:48 AM	
inetpub	File Folder		6/27/17 3:12 AM	6/27/17 3:12 AM	
PerfLogs	File Folder		8/22/13 8:52 AM	8/22/13 8:39 AM	
Program Files	File Folder		9/25/17 5:49 AM	8/22/13 6:36 AM	
Program Files (x86)	File Folder		9/25/17 5:48 AM	8/22/13 6:36 AM	
ProgramData	File Folder		9/24/17 11:20 PM	8/22/13 6:36 AM	
Restore	File Folder		9/26/17 9:33 AM	9/26/17 9:33 AM	
Users	File Folder		5/17/17 11:31 AM	8/22/13 6:36 AM	
VBRCatalog	File Folder		5/09/17 3:26 AM	5/09/17 3:23 AM	
Windows	File Folder		9/25/17 5:49 AM	8/22/13 6:36 AM	

Name	\\IOP-W2K12R2-V5\C:

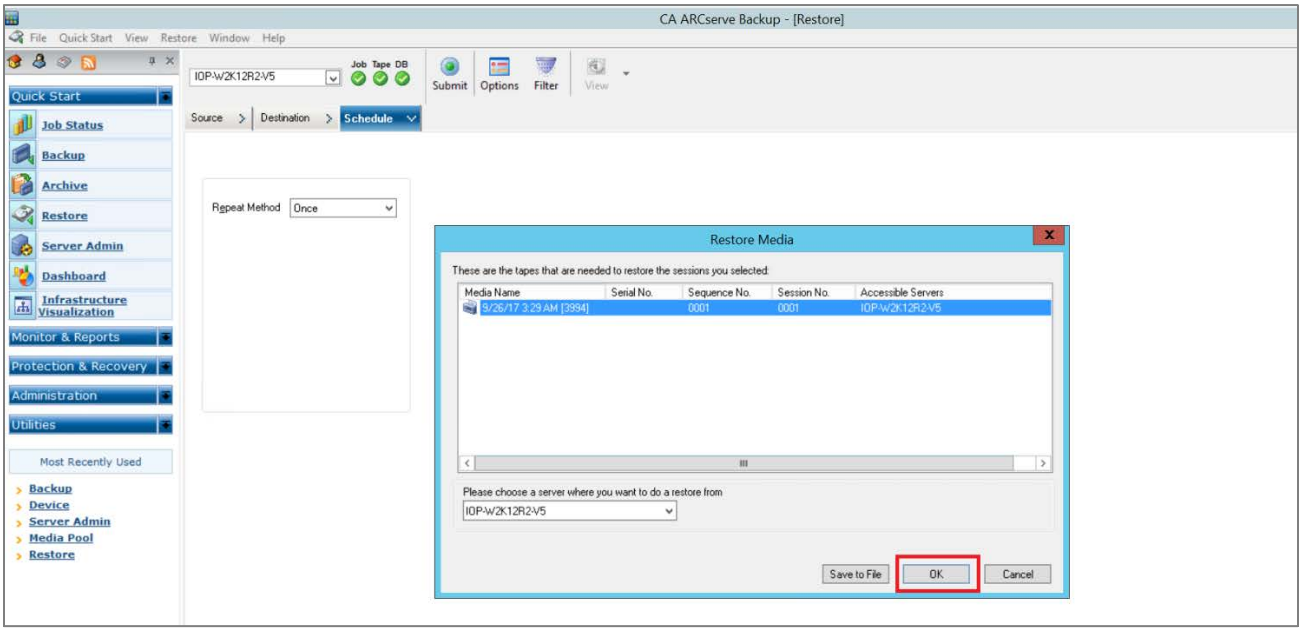
4 On the **Schedule** tab, select Repeat Method, and click **Submit**.



IOP-W2K12R2-V5

Repeat Method: Once

5 In the **Restore Media** window, select a server from where you want to restore, and click **OK**.



IOP-W2K12R2-V5

Repeat Method: Once

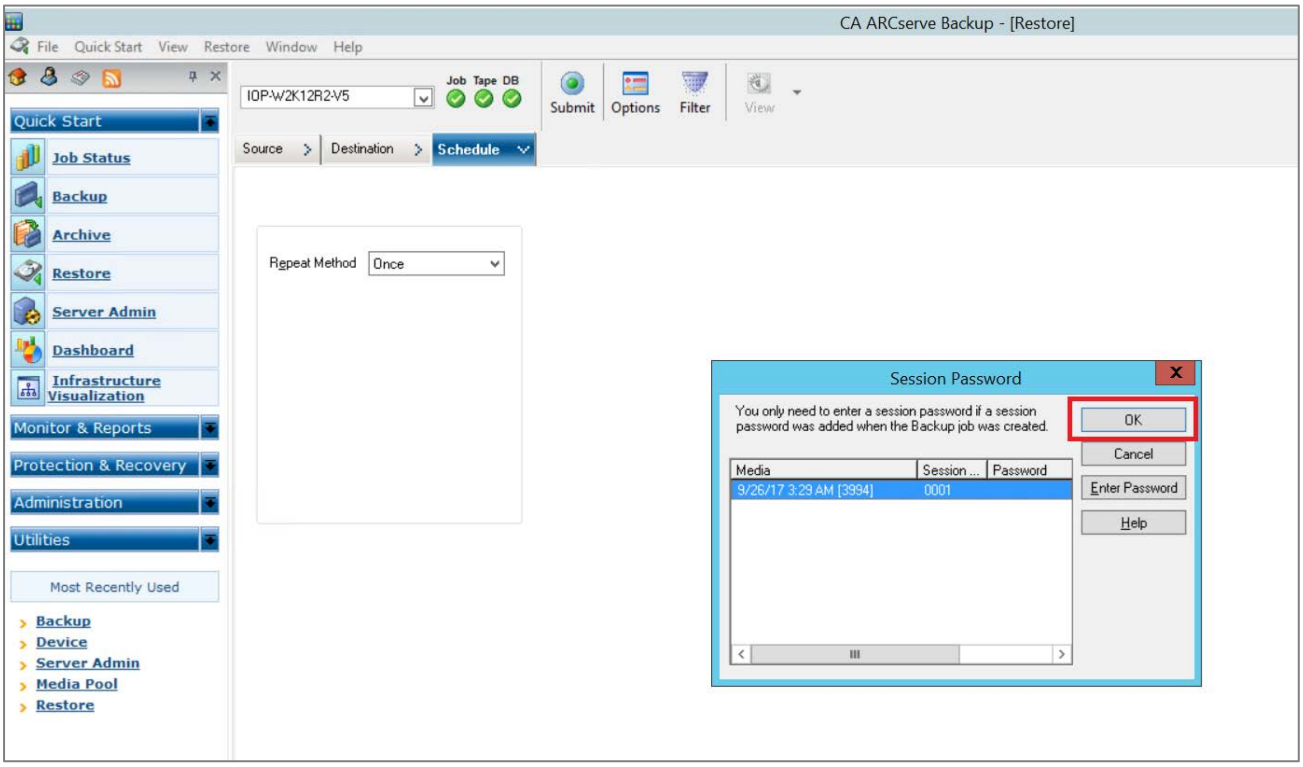
These are the tapes that are needed to restore the sessions you selected

Media Name	Serial No.	Sequence No.	Session No.	Accessible Servers
9/26/17 3:29 AM [3994]		0001	0001	IOP-W2K12R2-V5

Please choose a server where you want to do a restore from

IOP-W2K12R2-V5

6 In the **Session Password** window, click **OK**.



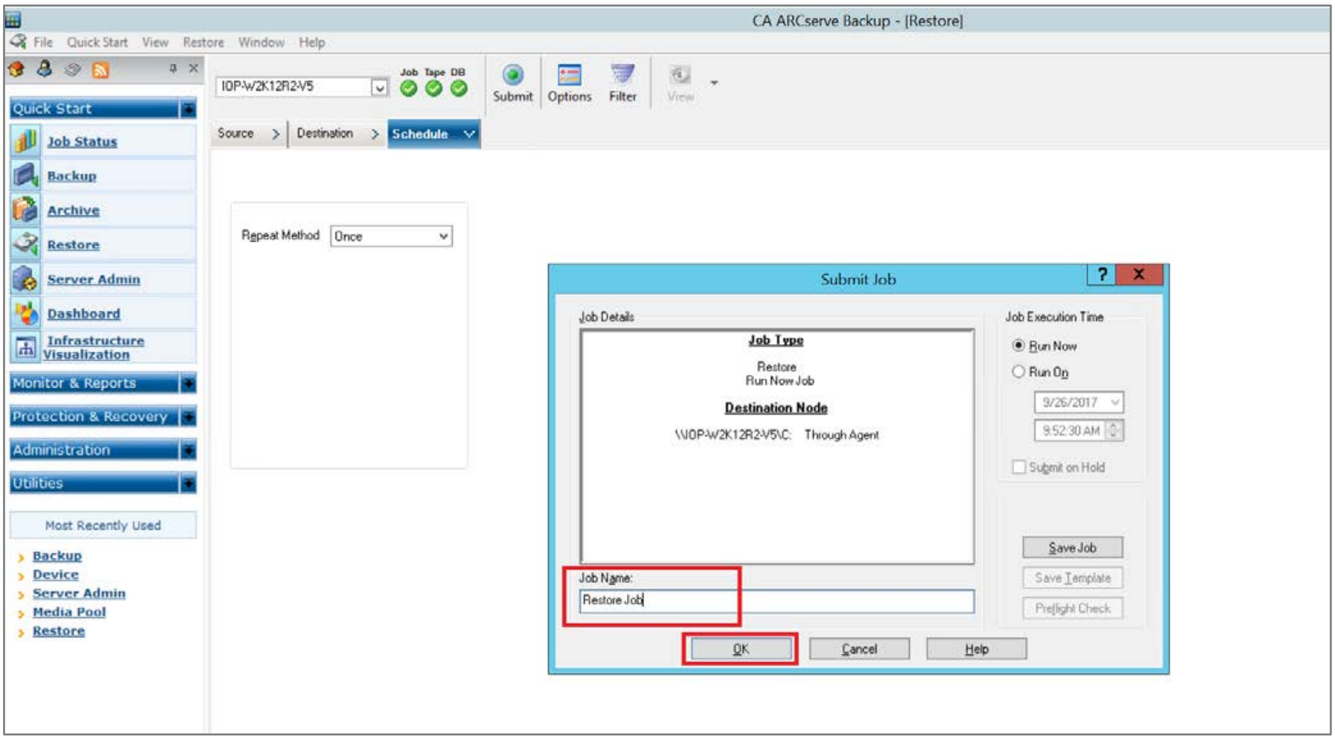
IOP-W2K12R2-V5

Repeat Method: Once

You only need to enter a session password if a session password was added when the Backup job was created.

Media	Session ...	Password
9/26/17 3:29 AM [3994]	0001	

7 In the **Submit Job** window, enter a Job Name, select a Job Execution Time, and click **OK**.



Repeat Method: Once

Submit Job

Job Details

Job Type

Restore
Run Now Job

Destination Node

\\IOP-W2K12R2-V5\C: Through Agent

Job Name: Restore Job

Job Execution Time

● Run Now

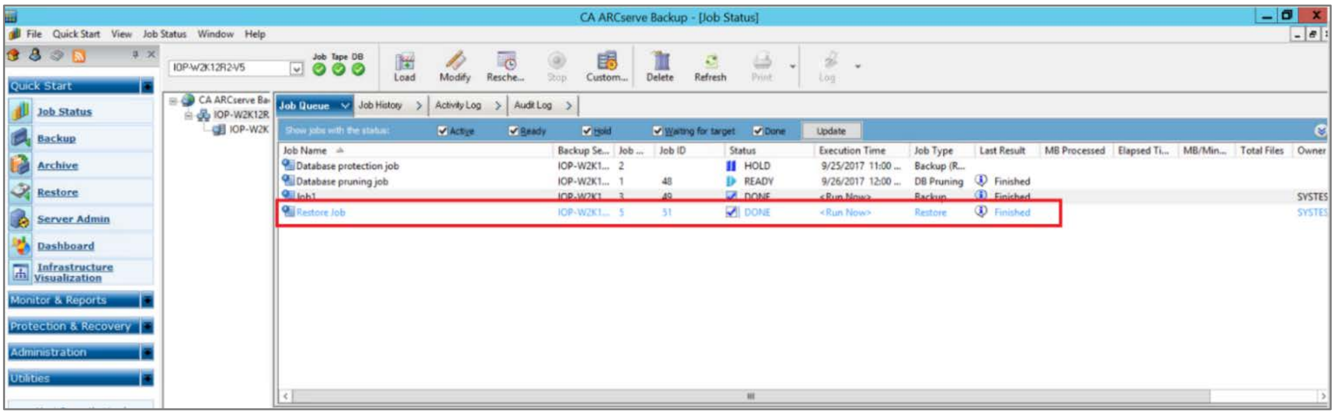
○ Run On

9/26/2017

9:52:30 AM

□ Submit on Hold

8 When the restore job runs, check the Job Queue display in the Job Status window.



Show jobs with the status: ☑ Active ☑ Ready ☑ Hold ☑ Waiting for target ☑ Done

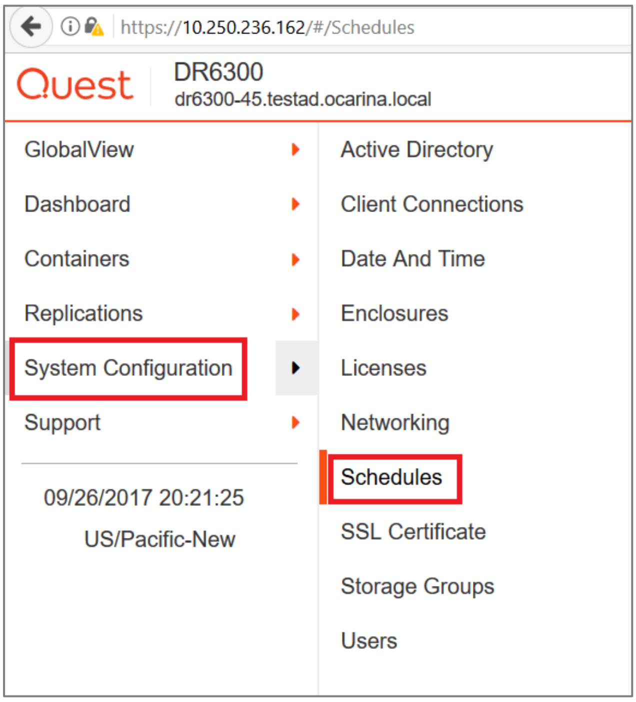
Job Name	Backup Se...	Job ...	Job ID	Status	Execution Time	Job Type	Last Result	MB Processed	Elapsed Ti...	MB/Min...	Total Files	Owner
Database protection job	IOP-W2K1...	2		HOLD	9/25/2017 11:00 ...	Backup (R...						
Database pruning job	IOP-W2K1...	1	48	READY	9/26/2017 12:00 ...	DB Pruning	Finished					
Job1	IOP-W2K1...	3	49	DONE	<Run Now>	Backup	Finished					SYSTES
Restore Job	IOP-W2K1...	5	51	DONE	<Run Now>	Restore	Finished					SYSTES

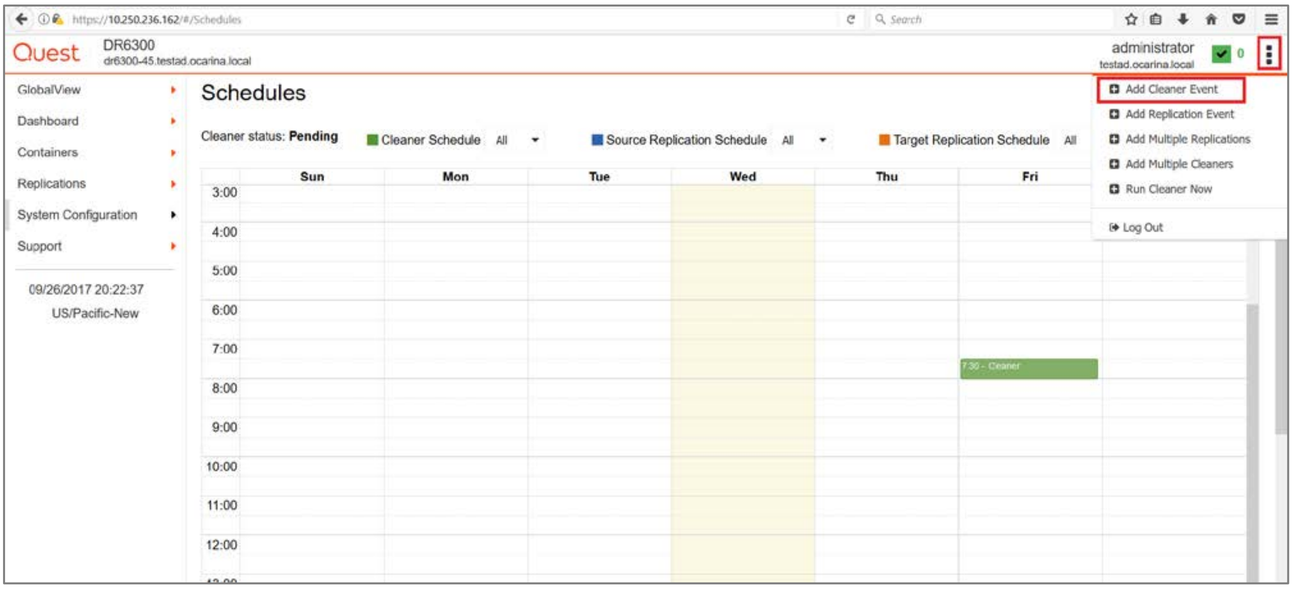
Setting up the system cleaner

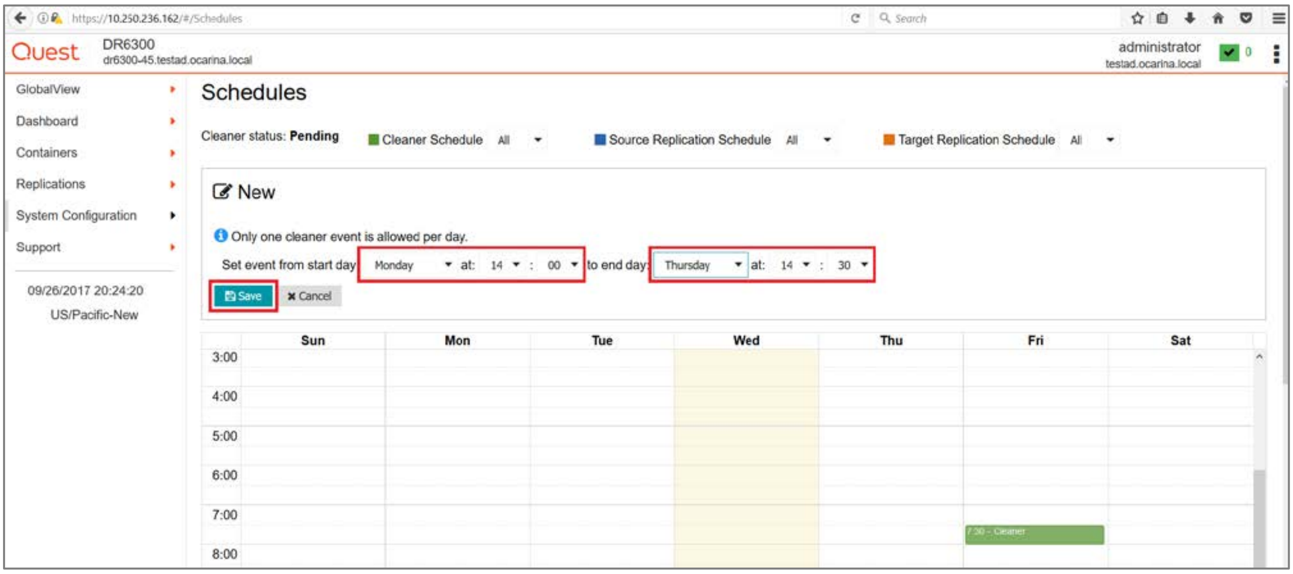
The cleaner will run during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner which will force it to run during that scheduled time.

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 setup the DR Series Deduplication Appliance cleaner can be scheduled. The DR Series Deduplication Appliance 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.







Only one cleaner event is allowed per day.

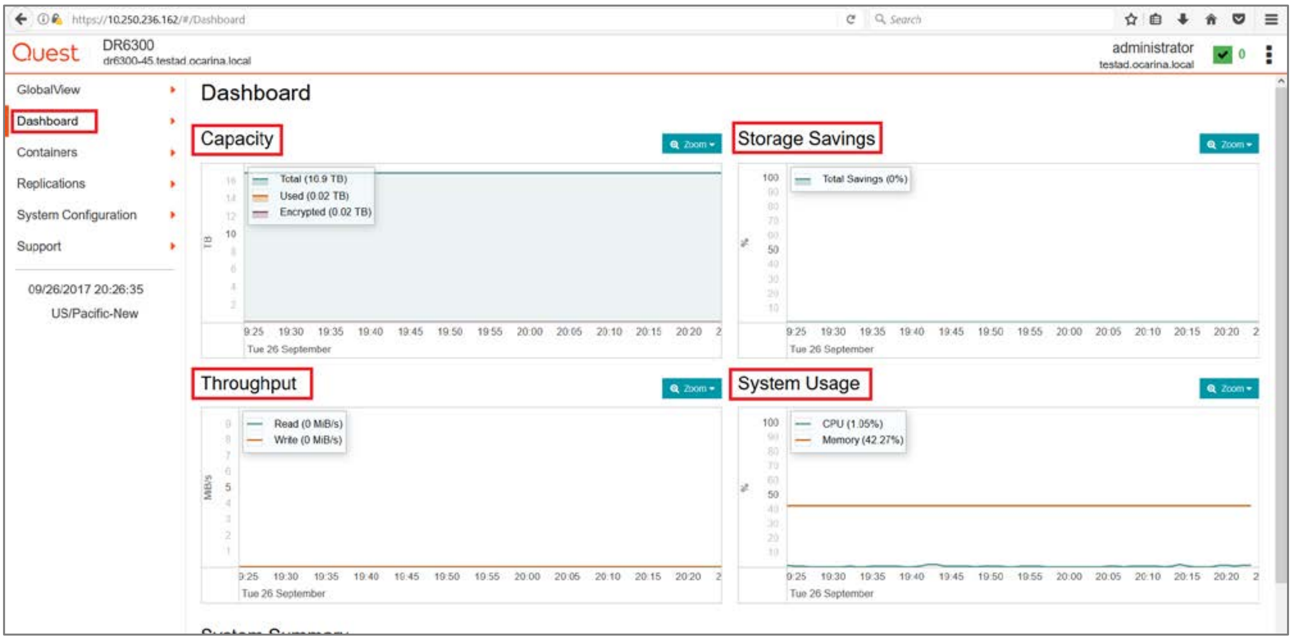
Set event from start day Monday at: 14 : 00 to end day Thursday at: 14 : 30

6

Monitoring deduplication, compression and performance

After backup jobs have completed, the DR Series Deduplication Appliance tracks capacity, storage savings and throughput on the DR Series Deduplication Appliance 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.



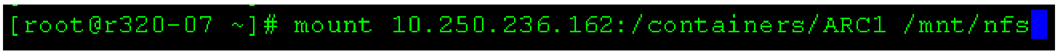
Appendices

A - Creating a storage device for NFS

For NFS backup using CA ARCserve, a target folder needs to be created as NFS share directory. This is the location to which backups will be written.

1. Mount the DR Series NFS share onto the NFS share directory to which the backup will be written in CA ARCserve.
2. Mount the NFS access path in the Linux agent server.

   Example:



```
[root@r320-07 ~]# mount 10.250.236.162:/containers/ARC1 /mnt/nfs
```