Setting Up Dell™ DR Series Deduplication Appliance Disk Backup Appliance on CA ARCserve

Dell Engineering
January 2014

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

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

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™ ,OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-0S®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

Table of contents

Revisions.. 2

Executive summary 4

1 Install and Configure the DR Series Deduplication Appliance Appliance.. 5

2 Set Up CA ARCserve..11

2.1 Procedure for the Windows Environment...11

2.2 Procedure for the Unix/Linux Environment 144

2.3 Procedure for restore from DR Replication…………………………………………………………………….15

3 Create a New Backup Job with DR Series Deduplication Appliance as the Target.................................... 15

4 Set Up the DR Series Deduplication Appliance Cleaner 22

5 Monitoring Deduplication, Compression and Performance 23

A Appendix..24

A.1 Create a Storage Device for NFS...24

Executive summary

This paper provides information about how to set up the Dell DR Series Deduplication Appliance as a backup target for CA ARCserve R16. This paper is a quick reference guide and does not include all DR Series Deduplication Appliance deployment best practices.

See the DR Series Deduplication Appliance documentation for other data management application best practices whitepapers at http://www.dell.com/support/troubleshooting/us/en/04/Product/powervault-dr4100, under "Manuals & Documentation".

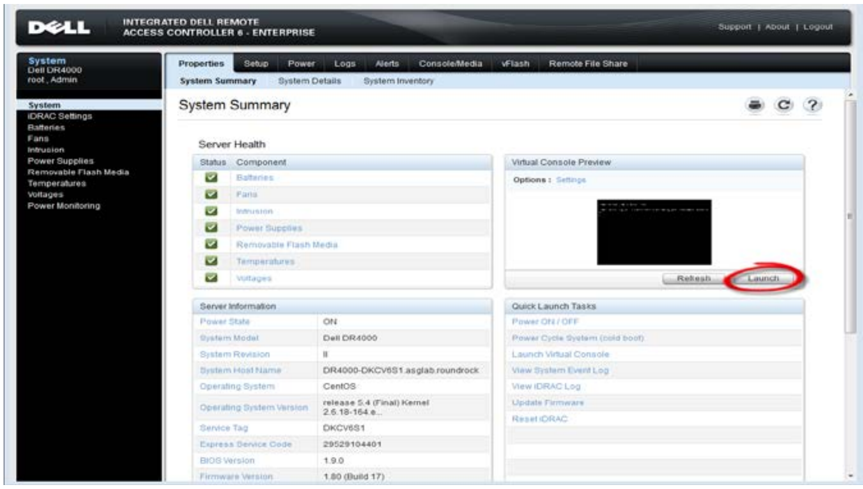
Note: The DR Series Deduplication Appliance/CA ARCserve build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series Deduplication Appliance/ CA ARCserve software version used.

1 Install and Configure the DR Series Deduplication Appliance

1. Rack and cable the DR Series Deduplication Appliance, and power it on.

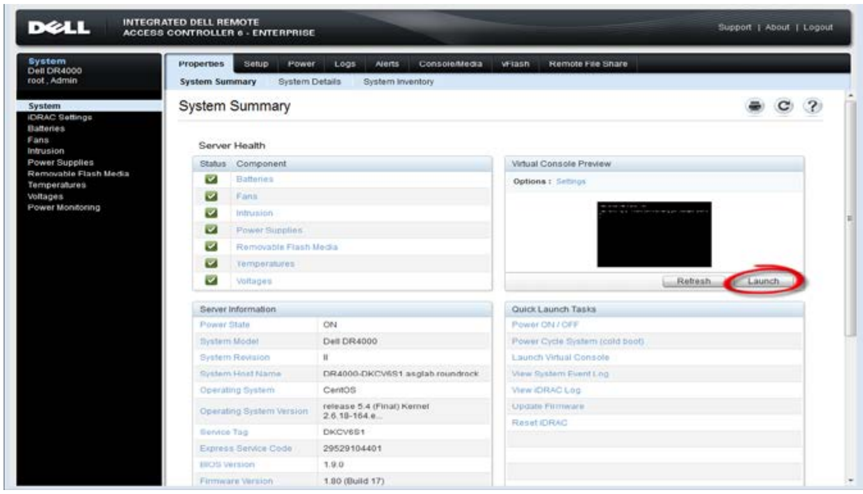
2. Please refer to *Dell DR Series System Administrator Guide*, under sections of "**iDRAC Connection**", "**Logging in and Initializing the DR Series System**", and "**Accessing IDRAC6/Idrac7 Using RACADM**" for using iDRAC connection and initializing the appliance.

3. Log in to iDRAC using the default address **192.168.0.120**, or the IP assigned to the iDRAC interface. Use user name and password of "**root/calvin**".



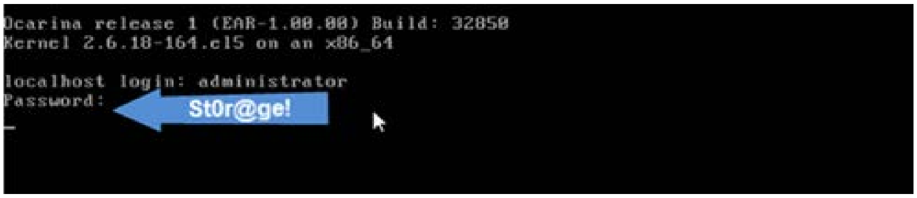
Server Information	
Power State	ON
System Model	Dell DR4000
System Revision	II
System Host Name	DR4000-DKCV6S1.asglab.roundrock
Operating System	CentOS
Operating System Version	release 5.4 (Final) Kernel 2.6.18-164.e...
Service Tag	DKCV6S1
Express Service Code	29529104401
BIOS Version	1.9.0
Firmware Version	1.80 (Build 17)

4. Launch the virtual console.



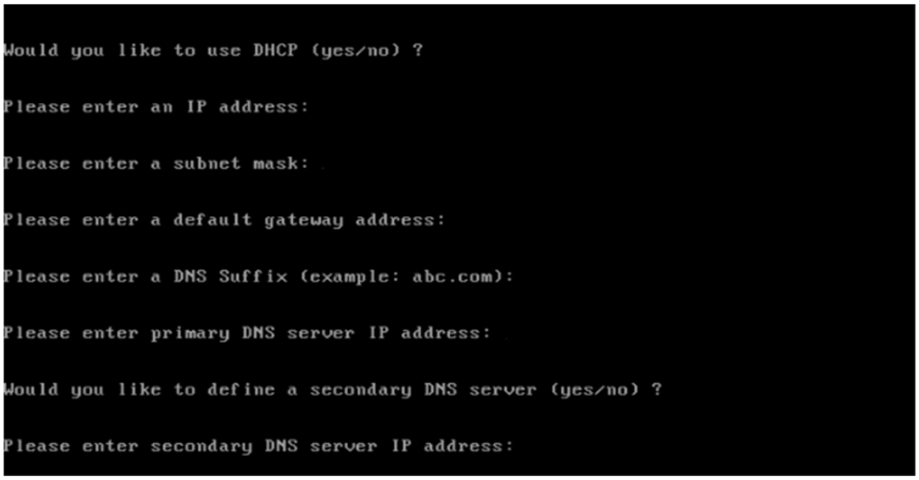
Server Information	
Power State	ON
System Model	Dell DR4000
System Revision	II
System Host Name	DR4000-DKCV6S1.asglab.roundrock
Operating System	CentOS
Operating System Version	release 5.4 (Final) Kernel 2.6.18-164.e...
Service Tag	DKCV6S1
Express Service Code	29529104401
BIOS Version	1.9.0
Firmware Version	1.80 (Build 17)

5. After the virtual console is open, log in to the system as user **administrator** and the password **St0r@ge!** (The "0" in the password is the numeral zero).



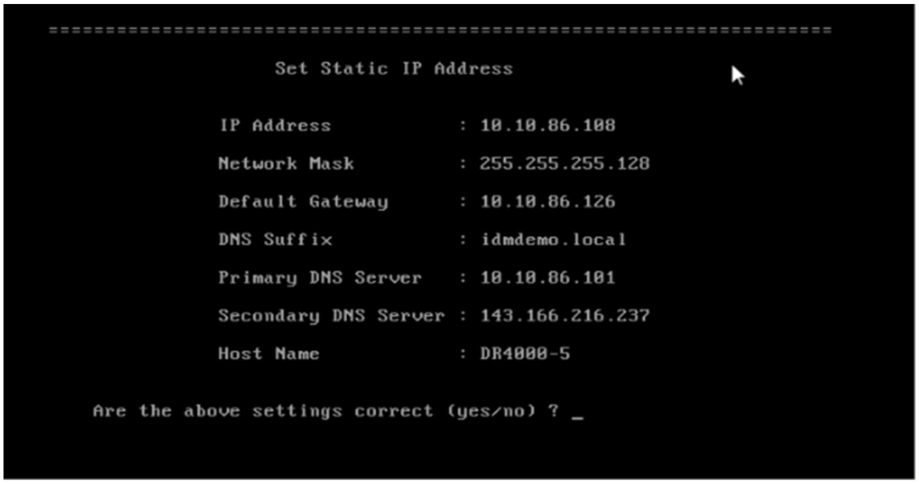
```
Ocarina release 1 (EAR-1.00.00) Build: 32850
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password:
_
```

6. Set the user-defined networking preferences.



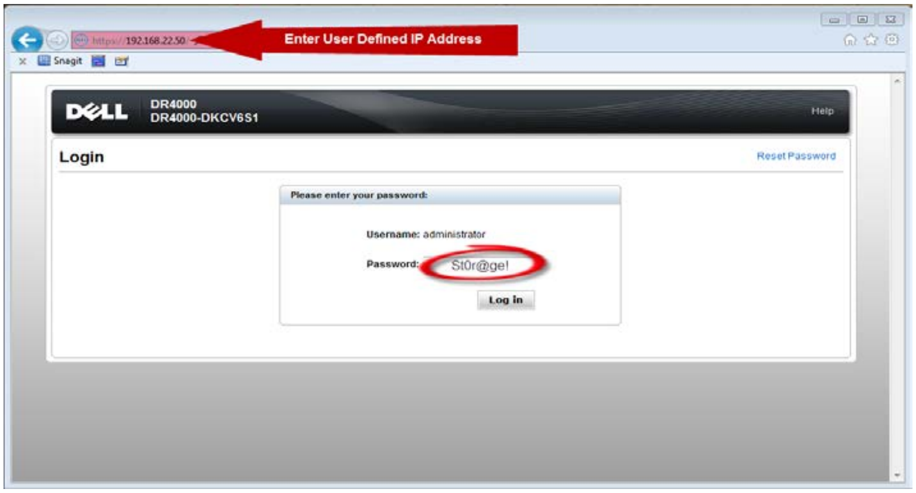
```
Would you like to use DHCP (yes/no) ?

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 DR Series Deduplication Appliance administrator console, using the IP address you just provided for the DR Series Deduplication Appliance, with username **administrator** and password **St0r@ge!** (The “0” in the password is the numeral zero.).



Enter User Defined IP Address

https://192.168.22.50/

DR4000
DR4000-DKCV6S1

Login

Please enter your password:

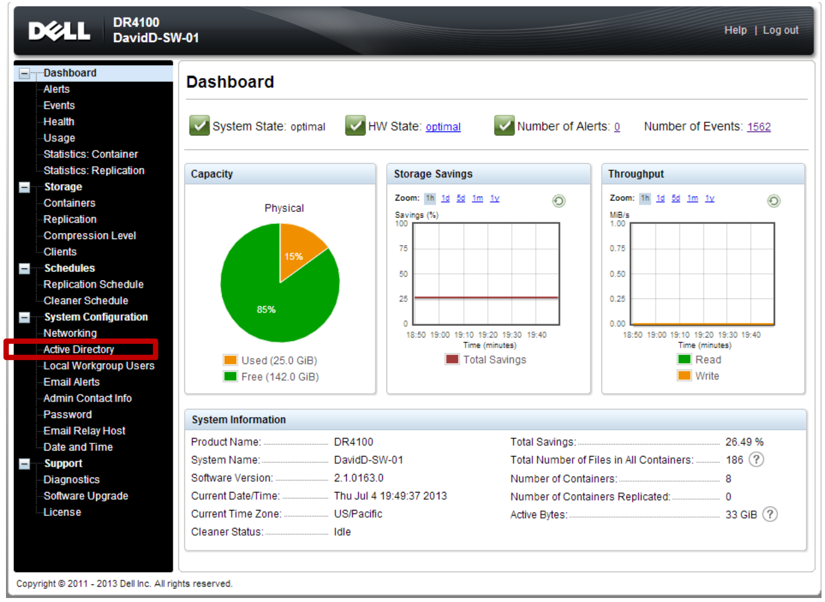
Username: administrator

Password: St0r@ge!

9. Join the DR Series Deduplication Appliance to Active Directory.

Note: if you do not want to add DR Series Deduplication Appliance to Active Directory, please see the *DR Series Deduplication Appliance Owner’s Manual* for guest login instructions.

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



DR4100
DavidD-SW-01

Dashboard

System State: optimal HW State: optimal Number of Alerts: 0 Number of Events: 1562

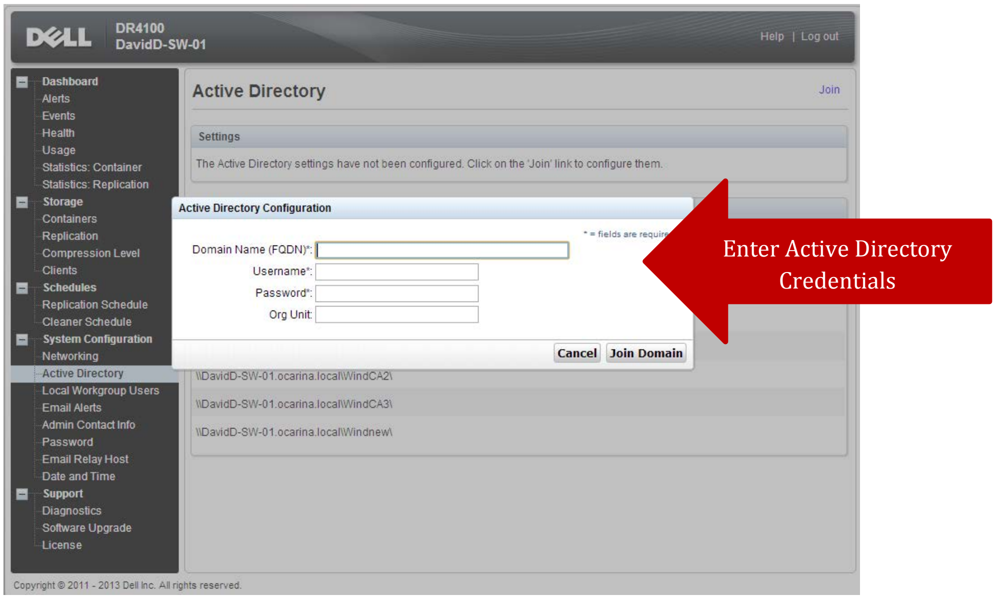
System Information

Product Name: DR4100
System Name: DavidD-SW-01
Software Version: 2.1.0163.0
Current Date/Time: Thu Jul 4 19:49:37 2013
Current Time Zone: US/Pacific
Cleaner Status: Idle

Total Savings: 26.49 %
Total Number of Files in All Containers: 186
Number of Containers: 8
Number of Containers Replicated: 0
Active Bytes: 33 GiB

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

- Enter your Active Directory credentials.



Active Directory

Settings

The Active Directory settings have not been configured. Click on the 'Join' link to configure them.

Active Directory Configuration

* = fields are require

Domain Name (FQDN)*:

Username*:

Password*:

Org Unit:

\\DavidD-SW-01.ocarina.local\WindCA2\

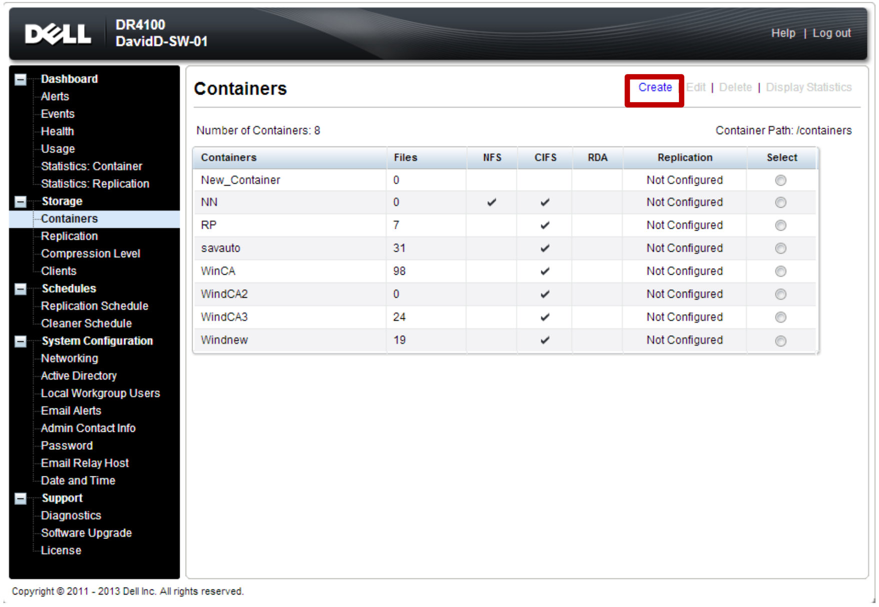
\\DavidD-SW-01.ocarina.local\WindCA3\

\\DavidD-SW-01.ocarina.local\Windnew\

Enter Active Directory Credentials

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

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



Containers

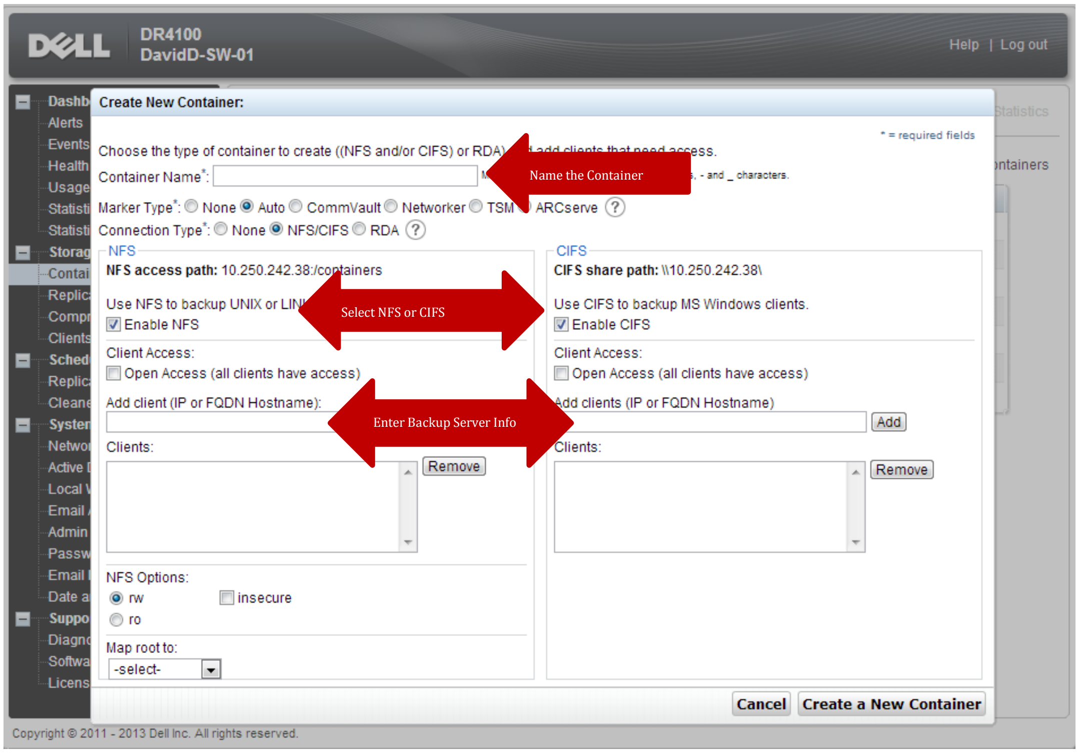
Number of Containers: 8

Container Path: /containers

Containers	Files	NFS	CIFS	RDA	Replication	Select
New_Container	0				Not Configured	○
NN	0	✓	✓		Not Configured	○
RP	7		✓		Not Configured	○
savauto	31		✓		Not Configured	○
WinCA	98		✓		Not Configured	○
WindCA2	0		✓		Not Configured	○
WindCA3	24		✓		Not Configured	○
Windnew	19		✓		Not Configured	○

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

11. Enter a **Container Name** and select the **Enable CIFS/NFS** check box.



Create New Container:

* = required fields

Choose the type of container to create ((NFS and/or CIFS) or RDA) ...d add clients that need access.

Container Name*: ... , - and _ characters.

Marker Type*: ○ None ● Auto ○ CommVault ○ Networker ○ TSM ○ ARCserve (?)

Connection Type*: ○ None ● NFS/CIFS ○ RDA (?)

NFS

NFS access path: 10.250.242.38:/containers

Use NFS to backup UNIX or LIN...

☑ Enable NFS

Client Access:

☐ Open Access (all clients have access)

Add client (IP or FQDN Hostname):

Clients:

NFS Options:

● rw ☐ insecure

○ ro

Map root to: -select-

CIFS

CIFS share path: \\10.250.242.38\

Use CIFS to backup MS Windows clients.

☑ Enable CIFS

Client Access:

☐ Open Access (all clients have access)

Add clients (IP or FQDN Hostname)

Clients:

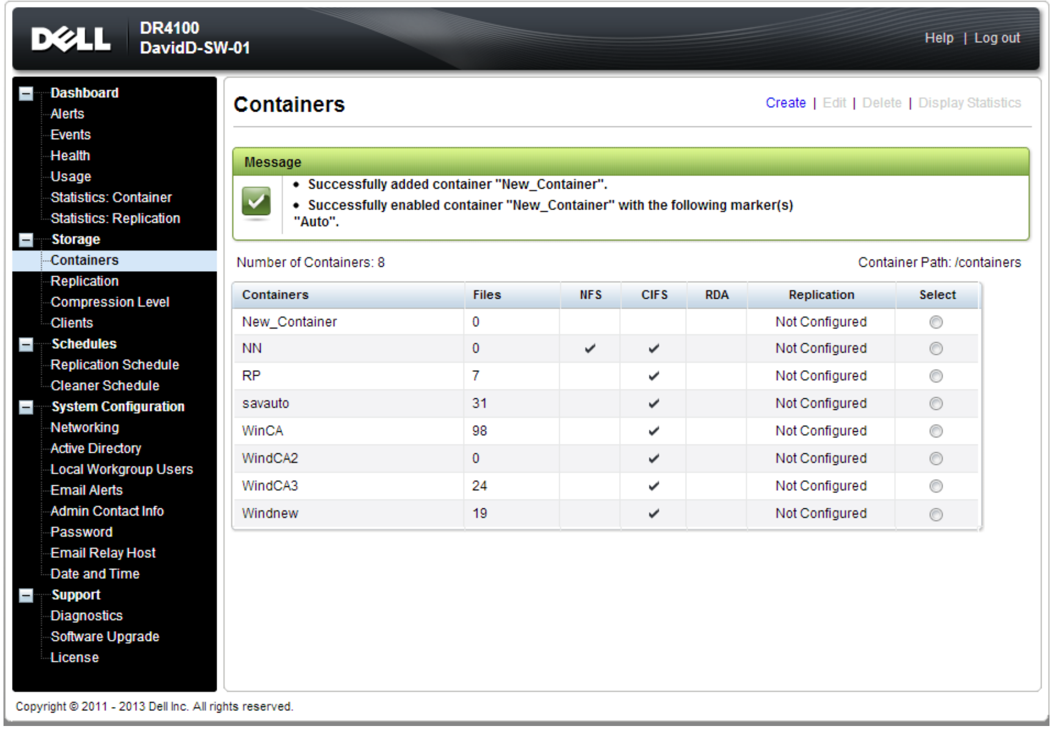
Name the Container

Select NFS or CIFS

Enter Backup Server Info

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

12. Click **Create a New Container**. Confirm that the container is added.



Containers

Message

- Successfully added container "New_Container".
- Successfully enabled container "New_Container" with the following marker(s) "Auto".

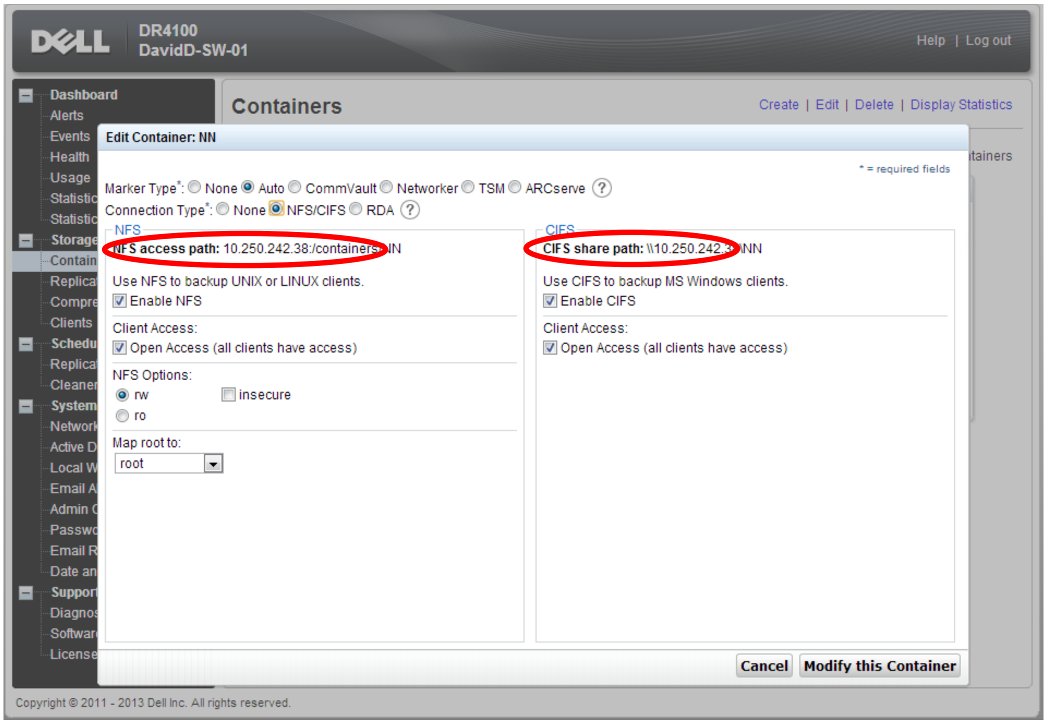
Number of Containers: 8

Container Path: /containers

Containers	Files	NFS	CIFS	RDA	Replication	Select
New_Container	0				Not Configured	○
NN	0	✓	✓		Not Configured	○
RP	7		✓		Not Configured	○
savauto	31		✓		Not Configured	○
WinCA	98		✓		Not Configured	○
WindCA2	0		✓		Not Configured	○
WindCA3	24		✓		Not Configured	○
Windnew	19		✓		Not Configured	○

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

13. Click **Edit.** Note down the container share/export path, which you will use later to target the DR Series Deduplication Appliance.



Edit Container: NN

* = required fields

Marker Type*: ○ None ● Auto ○ CommVault ○ Networker ○ TSM ○ ARCserve ?

Connection Type*: ○ None ● NFS/CIFS ○ RDA ?

NFS

NFS access path: 10.250.242.38:/containers/NN

Use NFS to backup UNIX or LINUX clients.

☑ Enable NFS

Client Access:

☑ Open Access (all clients have access)

NFS Options:

● rw ☐ insecure

○ ro

Map root to: root

CIFS

CIFS share path: \\10.250.242.38\NN

Use CIFS to backup MS Windows clients.

☑ Enable CIFS

Client Access:

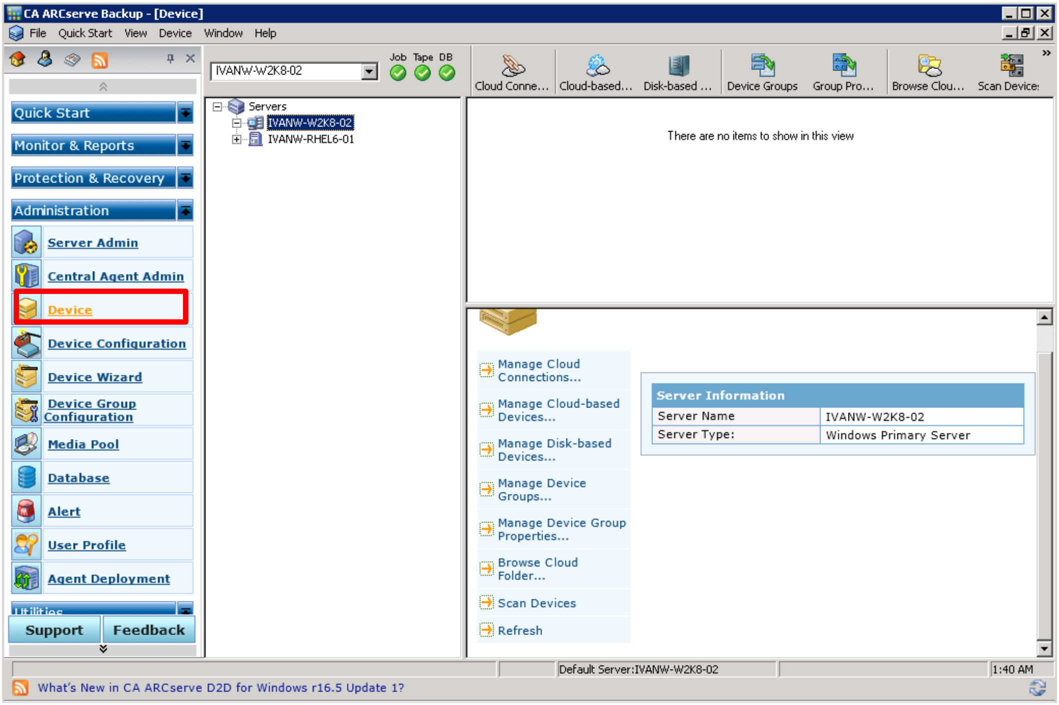
☑ Open Access (all clients have access)

14. Click Cancel to exit.

2 Create Disk-Based Target Device on CA ARCserve

2.1 Procedure for the Windows Environment

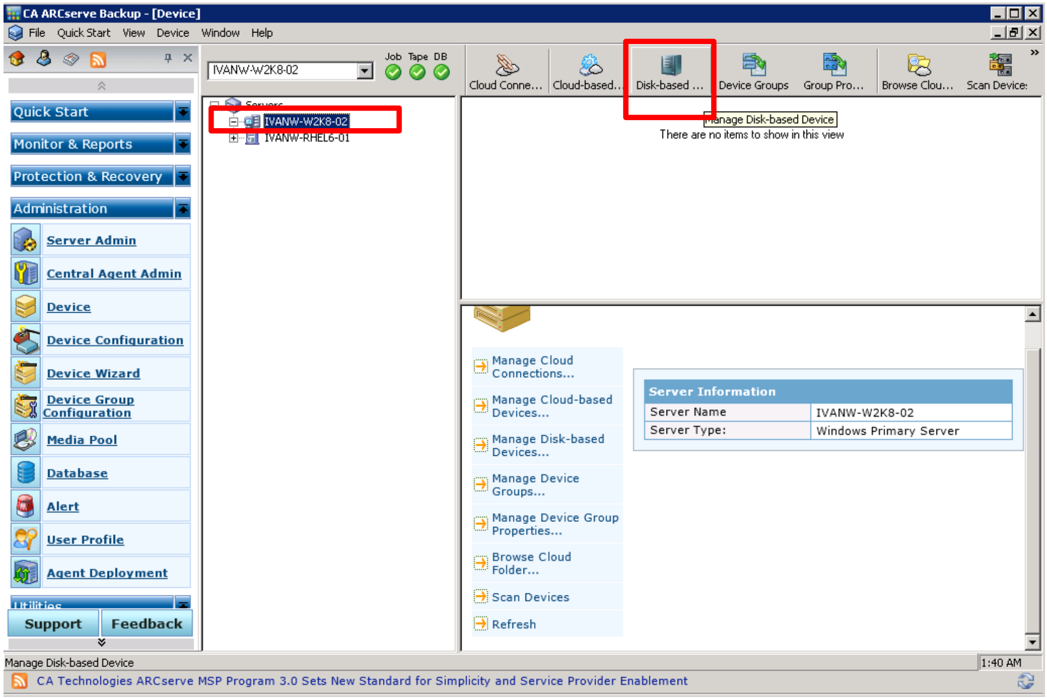
1. Open CA ARCserve Manager. In Navigation pane expand **Administration**, Click **Device**.



There are no items to show in this view

Server Information	
Server Name	IVANW-W2K8-02
Server Type:	Windows Primary Server

2. Select a **Server** -> Click **Disk-Based Device**



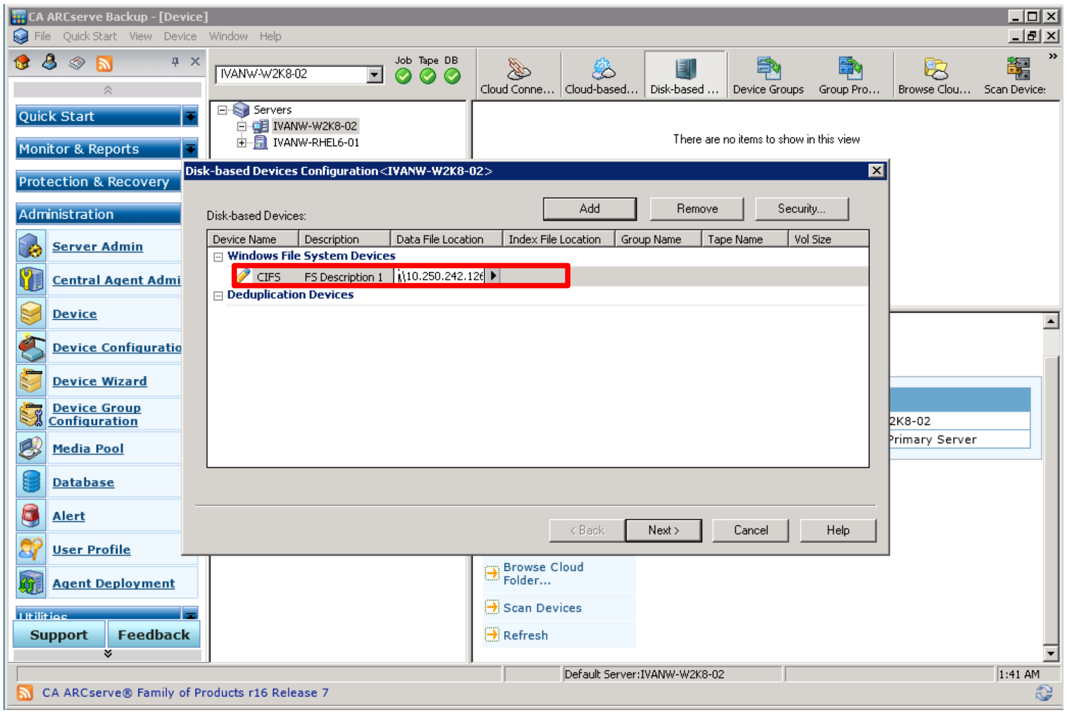
There are no items to show in this view

Server Information	
Server Name	IVANW-W2K8-02
Server Type:	Windows Primary Server

Manage Disk-based Device

CA Technologies ARCserve MSP Program 3.0 Sets New Standard for Simplicity and Service Provider Enablement

3. Select **Windows File System Devices** ->Enter a **Device name**, **Description**, DR container share path as **Data File Location**.



There are no items to show in this view

Disk-based Devices Configuration<IVANW-W2K8-02>

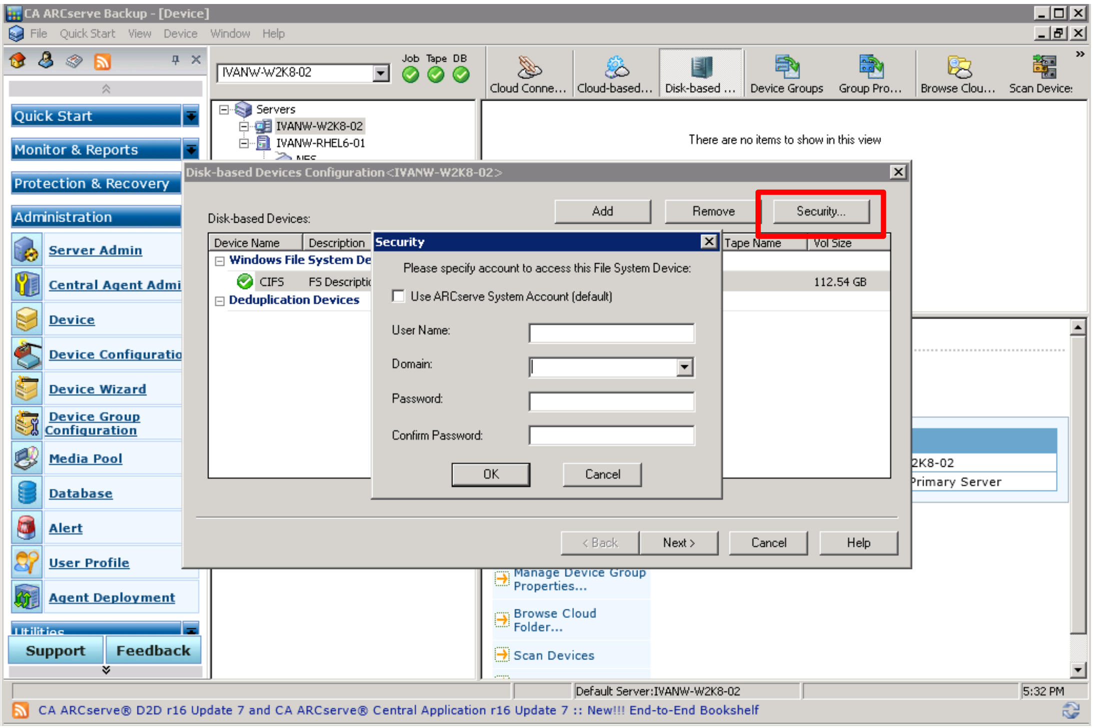
Disk-based Devices:

Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vol Size
Windows File System Devices						
CIFS	FS Description 1	\\10.250.242.126				
Deduplication Devices						

Default Server:IVANW-W2K8-02

CA ARCserve® Family of Products r16 Release 7

4. 2.1.4 Click on **Security...** Enter credentials of domain , click **OK**



Device Name	Description	Tape Name	Vol Size
Windows File System De			
CIFS	FS Descripti		112.54 GB
Deduplication Devices			

Security

Please specify account to access this File System Device:

□ Use ARCserve System Account (default)

User Name:

Domain:

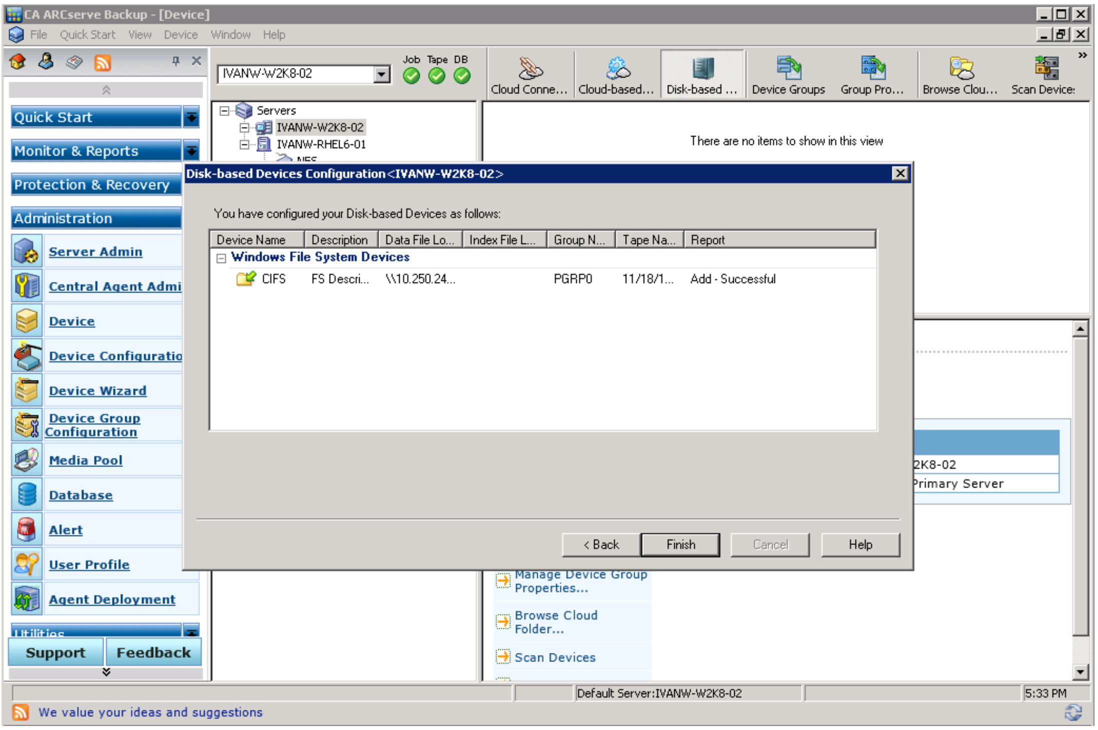
Password:

Confirm Password:

OK Cancel

CA ARCserve® D2D r16 Update 7 and CA ARCserve® Central Application r16 Update 7 :: New!!! End-to-End Bookshelf

5. Click **Finish**.



You have configured your Disk-based Devices as follows:

Device Name	Description	Data File Lo...	Index File L...	Group N...	Tape Na...	Report
Windows File System Devices						
CIFS	FS Descri...	\\10.250.24...		PGRP0	11/18/1...	Add - Successful

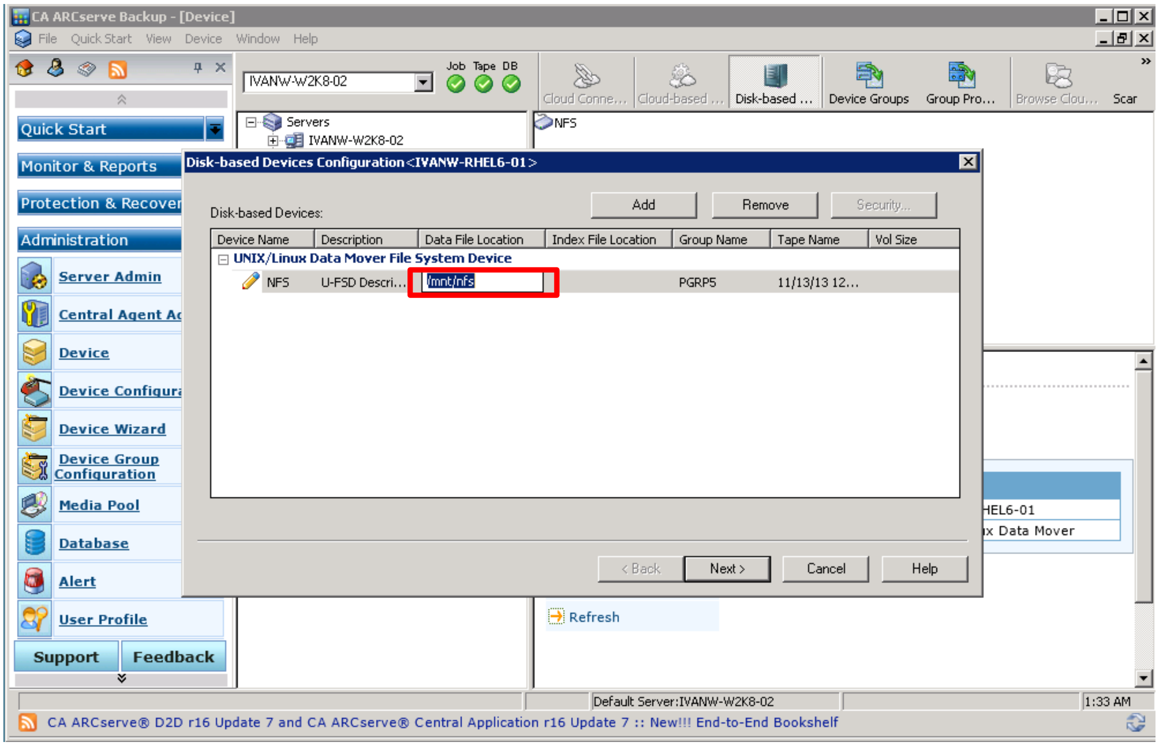
We value your ideas and suggestions

2.2 Procedure for the Unix/Linux Environment

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.

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 **Data File Location**.

For other details, please refer to 2.1 Procedure for the Windows Environment.



Disk-based Devices Configuration<IVANW-RHEL6-01>

Disk-based Devices:

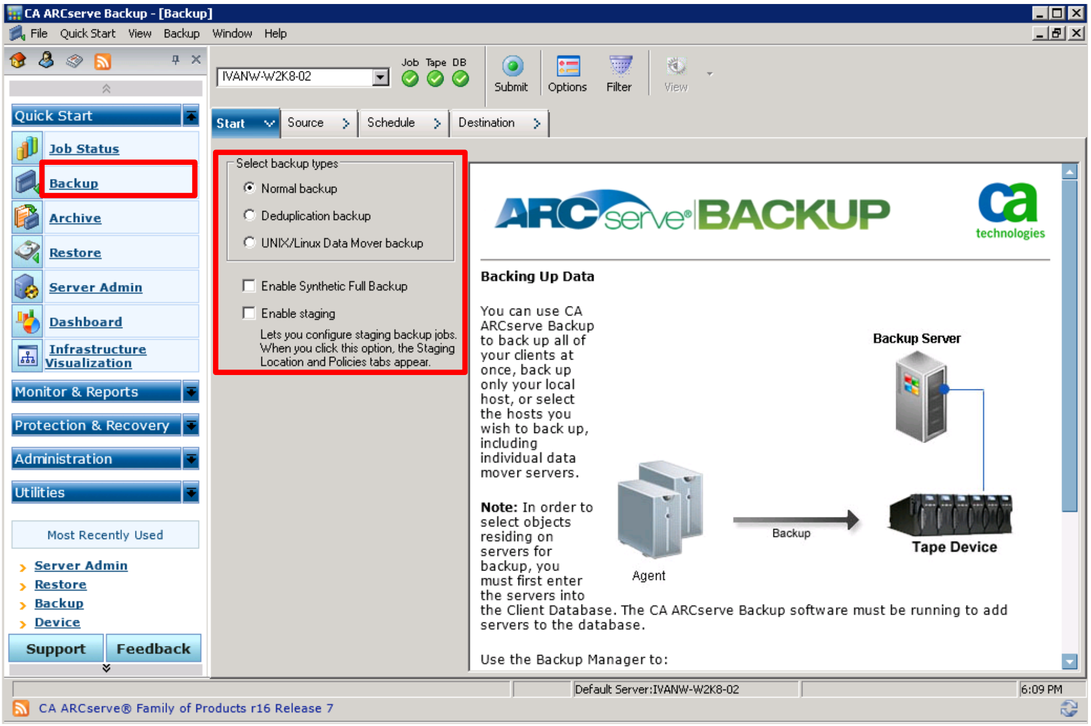
Add | Remove | Security...

Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vol Size
UNIX/Linux Data Mover File System Device						
NFS	U-FSD Descri...	/mnt/nfs		PGRP5	11/13/13 12...	

< Back | Next > | Cancel | Help

3 Create a New Backup Job with DR Series Deduplication Appliance as the Target

1. In the Navigation pane, click **Quick start** -> **Backup**. Then in right side panel, on **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.

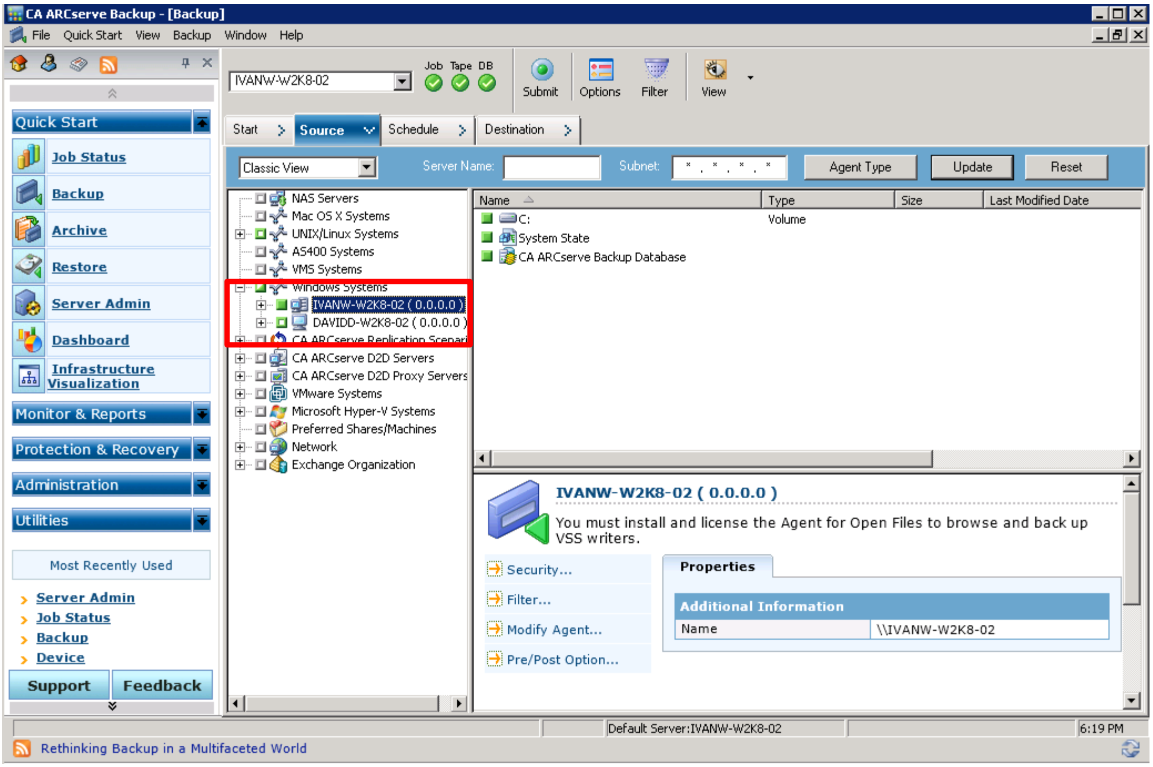
Backing Up Data

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:

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

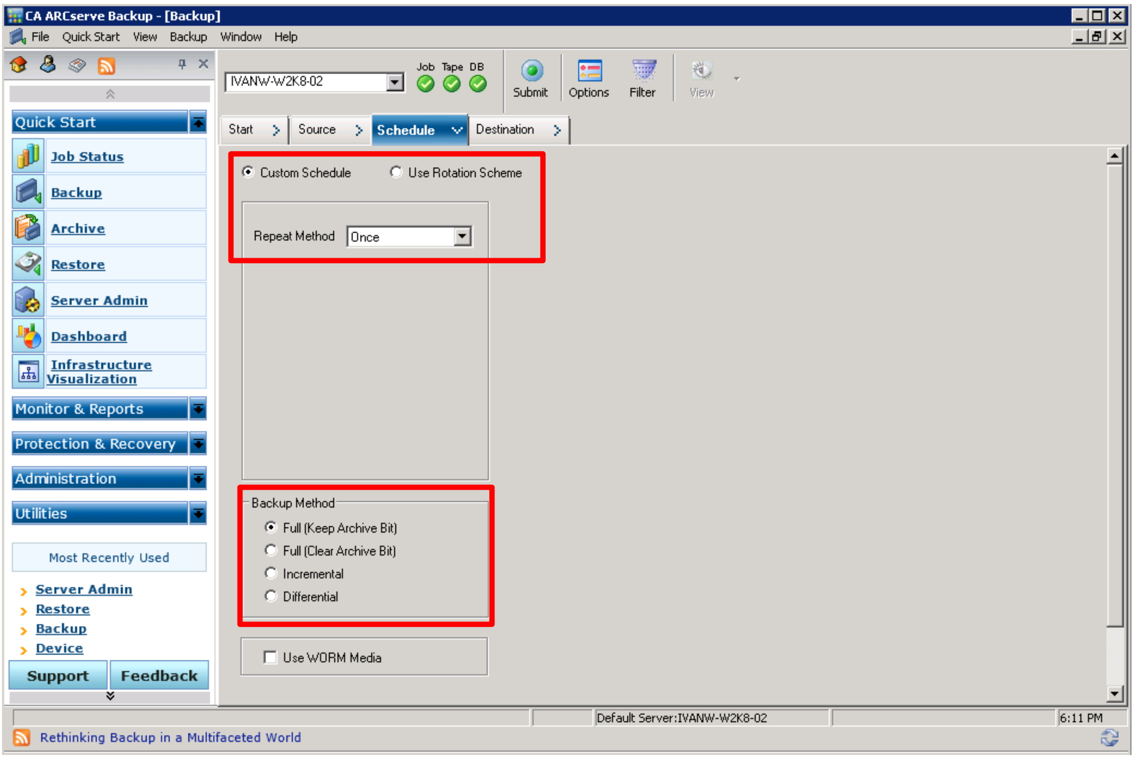


IVANW-W2K8-02 (0.0.0.0)

You must install and license the Agent for Open Files to browse and back up VSS writers.

Name	\\IVANW-W2K8-02

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



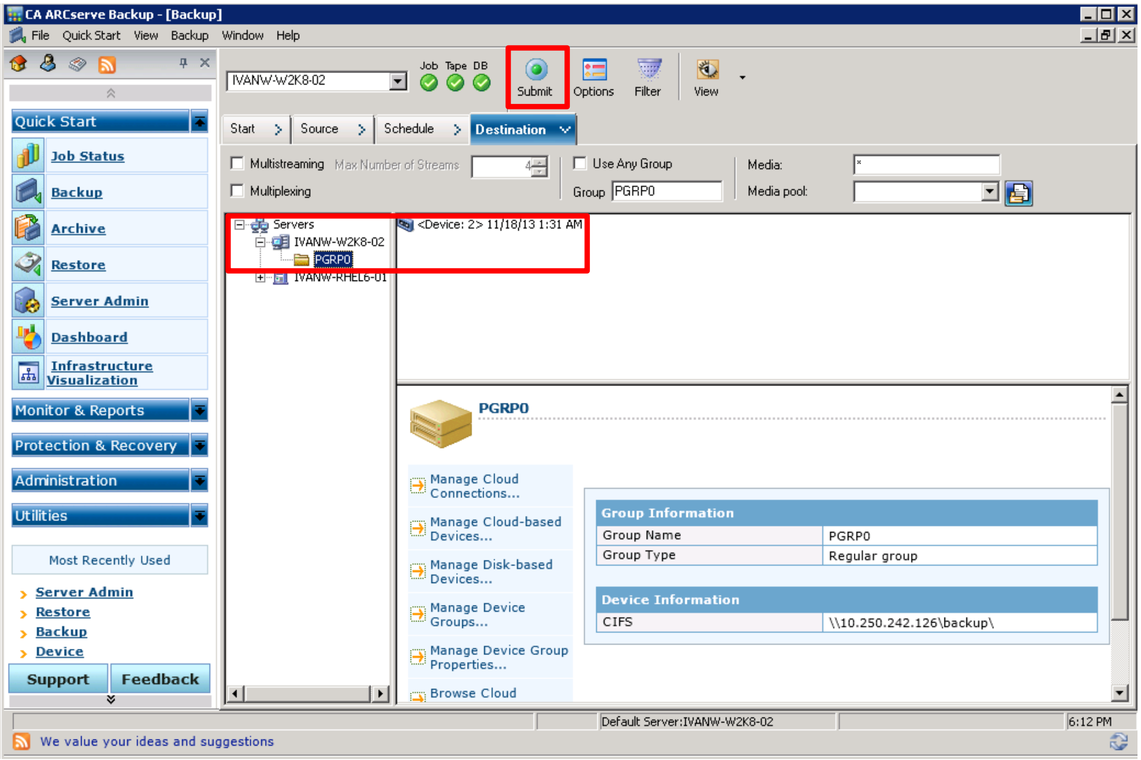
● Custom Schedule ○ Use Rotation Scheme

Repeat Method: Once

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

□ Use WORM Media

4. On **Destination** tab, select destination device that is created on DR. Click **Submit**.



□ Multistreaming Max Number of Streams 4

□ Multiplexing

□ Use Any Group

Group: PGRP0

Media: *

Media pool:

Servers
- IVANW-W2K8-02
  - PGRP0
- IVANW-RHEL6-01

<Device: 2> 11/18/13 1:31 AM

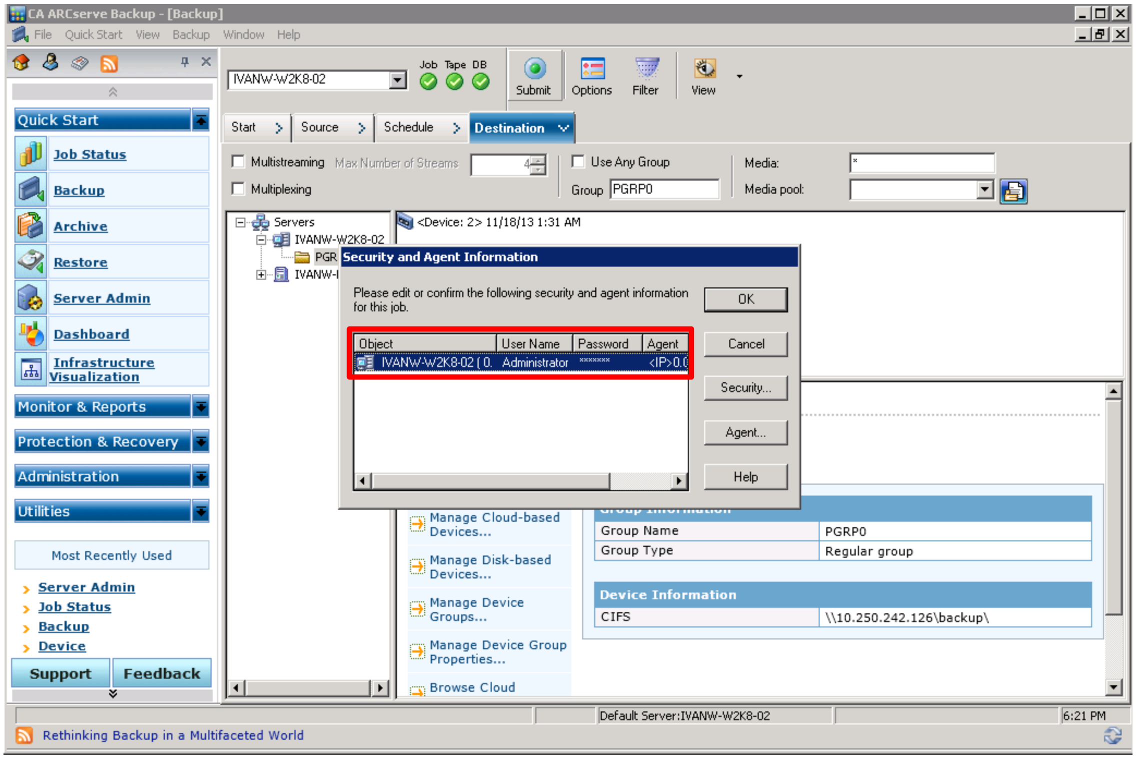
PGRP0

Group Information	
Group Name	PGRP0
Group Type	Regular group

Device Information	
CIFS	\\10.250.242.126\backup\

Default Server:IVANW-W2K8-02 6:12 PM

5. In **Security and Agent Information** window, choose an agent server, click **OK**.



□ Multistreaming Max Number of Streams 4

□ Multiplexing

□ Use Any Group

Group: PGRP0

Media: *

Media pool:

Servers
- IVANW-W2K8-02
  - PGR
- IVANW-I

<Device: 2> 11/18/13 1:31 AM

Security and Agent Information

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

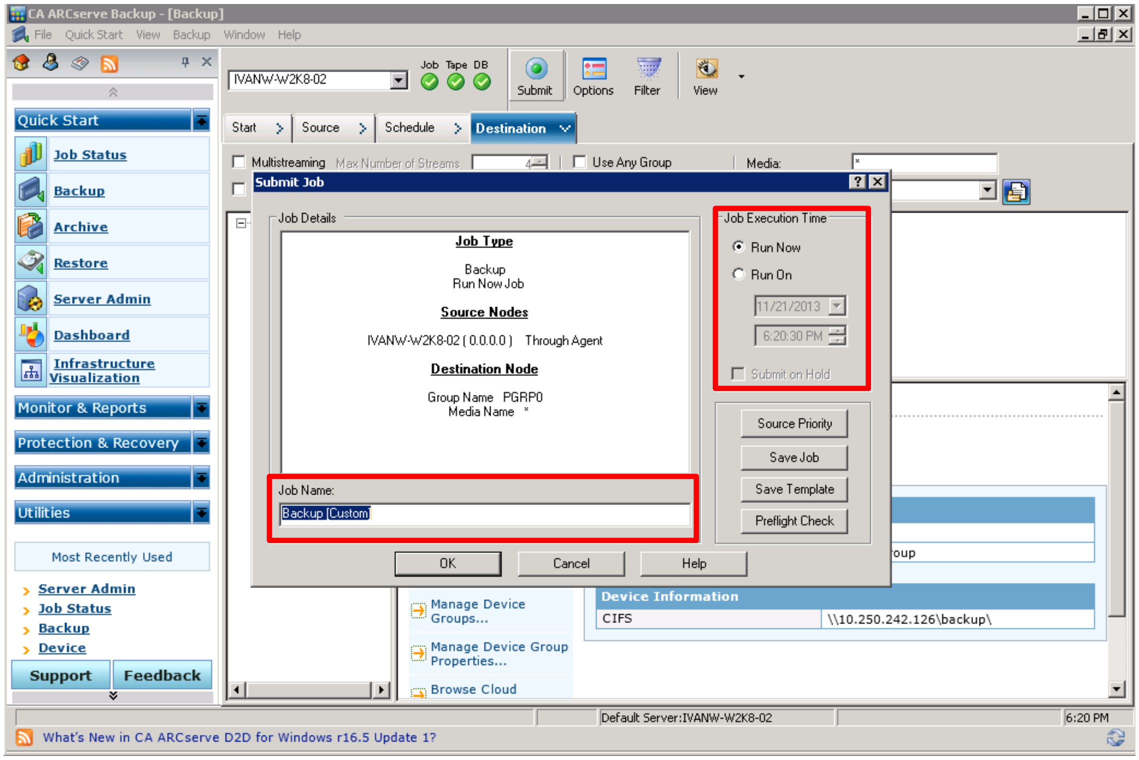
Object	User Name	Password	Agent
IVANW-W2K8-02 (0.	Administrator	*******	<IP>0.0

Group Information	
Group Name	PGRP0
Group Type	Regular group

Device Information	
CIFS	\\10.250.242.126\backup\

Default Server:IVANW-W2K8-02 6:21 PM

6. Enter the backup **Job Name**, choose **Job Execution Time**, then click **OK.**



Submit Job

Job Details

Job Type

Backup
Run Now Job

Source Nodes

IVANW-W2K8-02 (0.0.0.0) Through Agent

Destination Node

Group Name PGRP0
Media Name *

Job Name: Backup [Custom]

Job Execution Time

● Run Now

○ Run On

11/21/2013

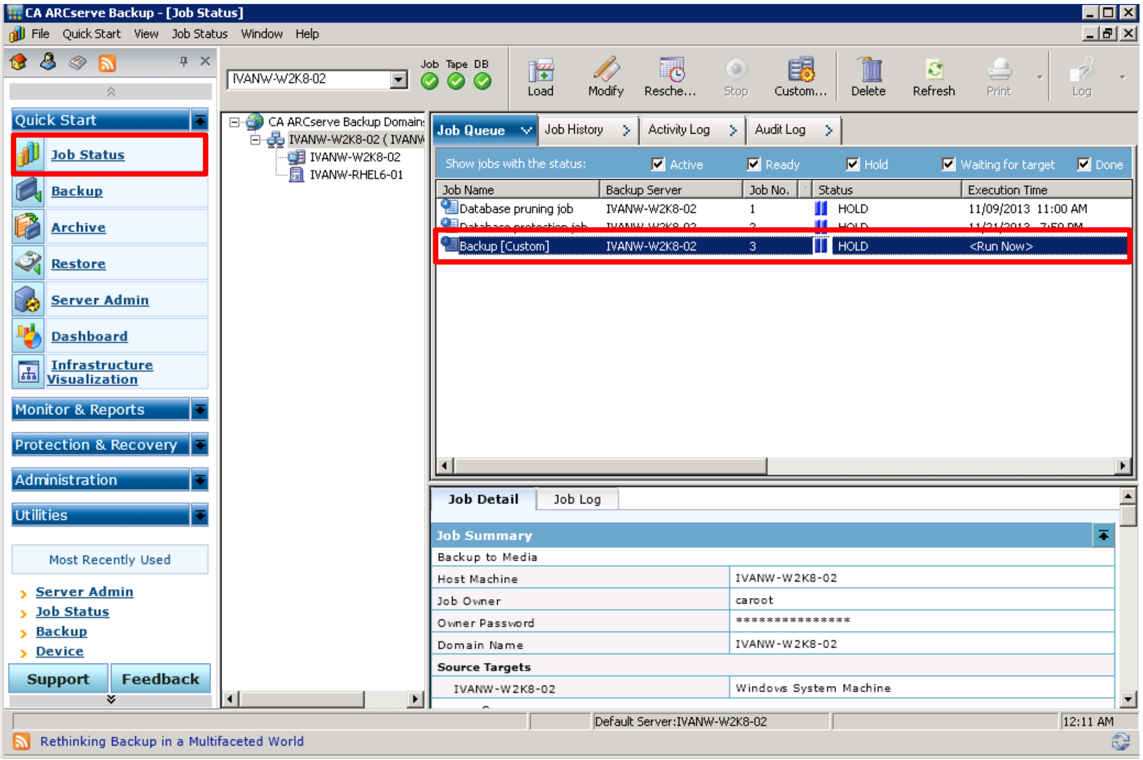
6:20:30 PM

□ Submit on Hold

Device Information

CIFS	\\10.250.242.126\backup\

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



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

Job Name	Backup Server	Job No.	Status	Execution Time
Database pruning job	IVANW-W2K8-02	1	HOLD	11/09/2013 11:00 AM
Database protection job	IVANW-W2K8-02	2	HOLD	11/21/2013 7:59 PM
Backup [Custom]	IVANW-W2K8-02	3	HOLD	<Run Now>

Job Summary

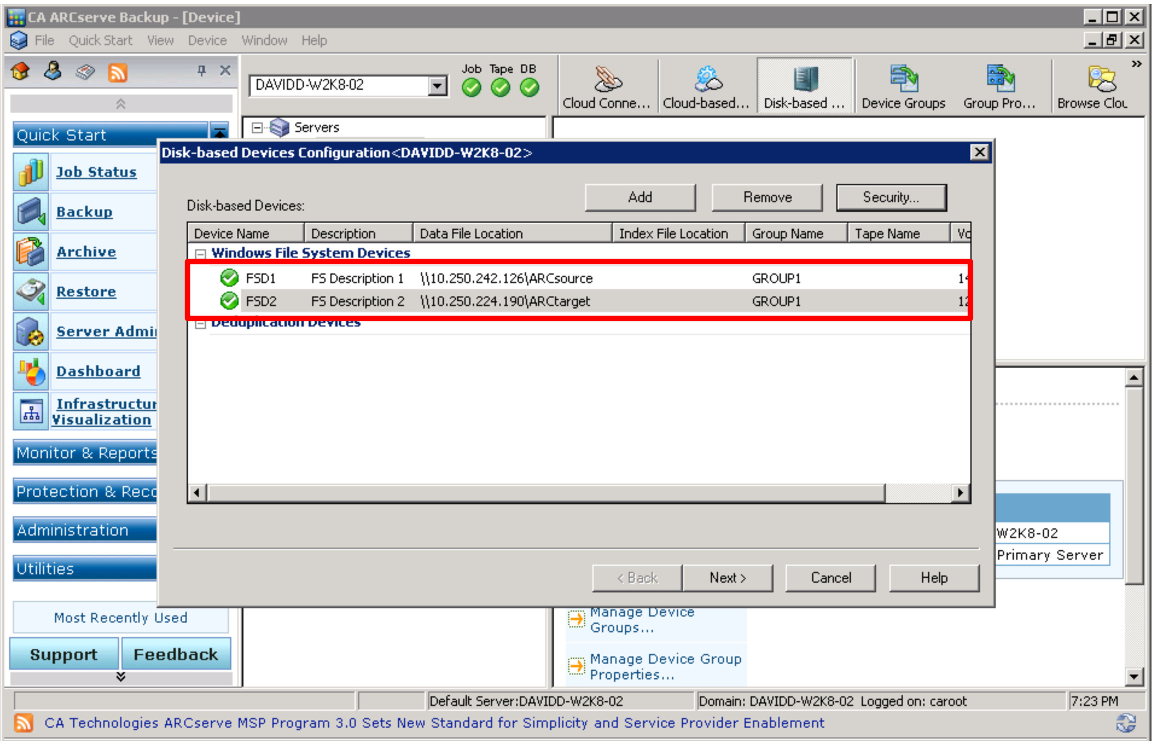
Backup to Media	
Host Machine	IVANW-W2K8-02
Job Owner	caroot
Owner Password	***************
Domain Name	IVANW-W2K8-02
Source Targets	
IVANW-W2K8-02	Windows System Machine

4 Set up DR Native Replication & Restore from Replication Target

Note: Assume DR1 is the replication source DR appliance, and DR2 is the replication target DR appliance. ‘ARCsource’ is the replication source container, and ‘ARCtarget’ is the replication target container.

4.1 Create DR Native Replication Session

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



Disk-based Devices Configuration<DAVIDD-W2K8-02>

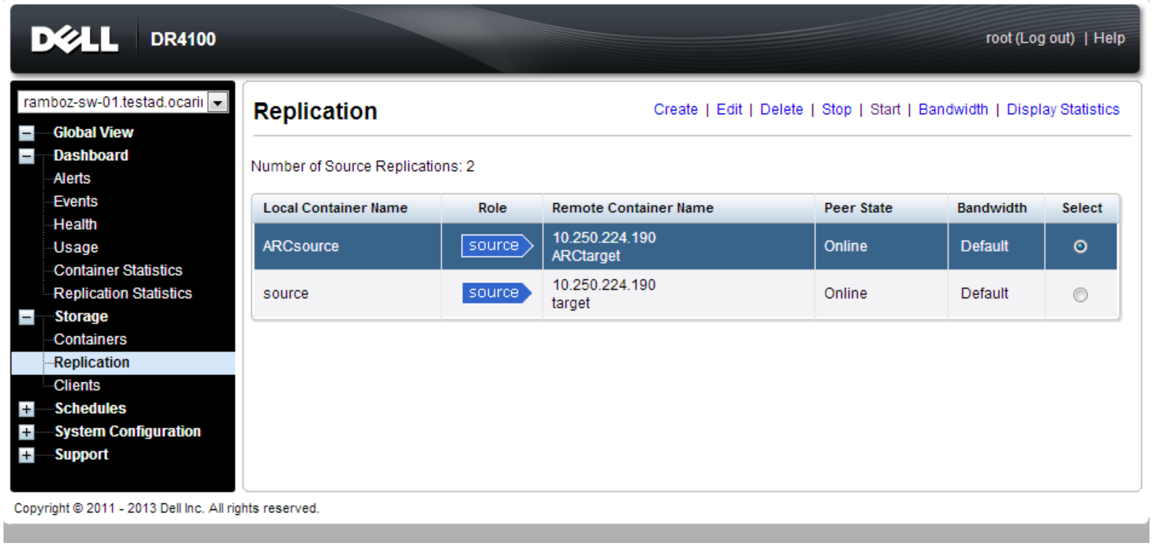
Disk-based Devices:

Device Name	Description	Data File Location	Index File Location	Group Name	Tape Name	Vo
Windows File System Devices						
✓ FSD1	FS Description 1	\\10.250.242.126\ARCsource		GROUP1		14
✓ FSD2	FS Description 2	\\10.250.224.190\ARCtarget		GROUP1		12
Deduplication Devices						

Default Server:DAVIDD-W2K8-02 Domain: DAVIDD-W2K8-02 Logged on: caroot 7:23 PM

CA Technologies ARCserve MSP Program 3.0 Sets New Standard for Simplicity and Service Provider Enablement

2. From DR1's GUI management interface, under **Replication** menu, click on **Create**. Set 'ARCsource' container as replication source, set DR2 'ARCtarget' container as replication target. **Start** the replication session, or make sure the replication session is **Online**. You can **Stop** and/or **Delete** the replication whenever it’s in INSYNC mode.



Replication

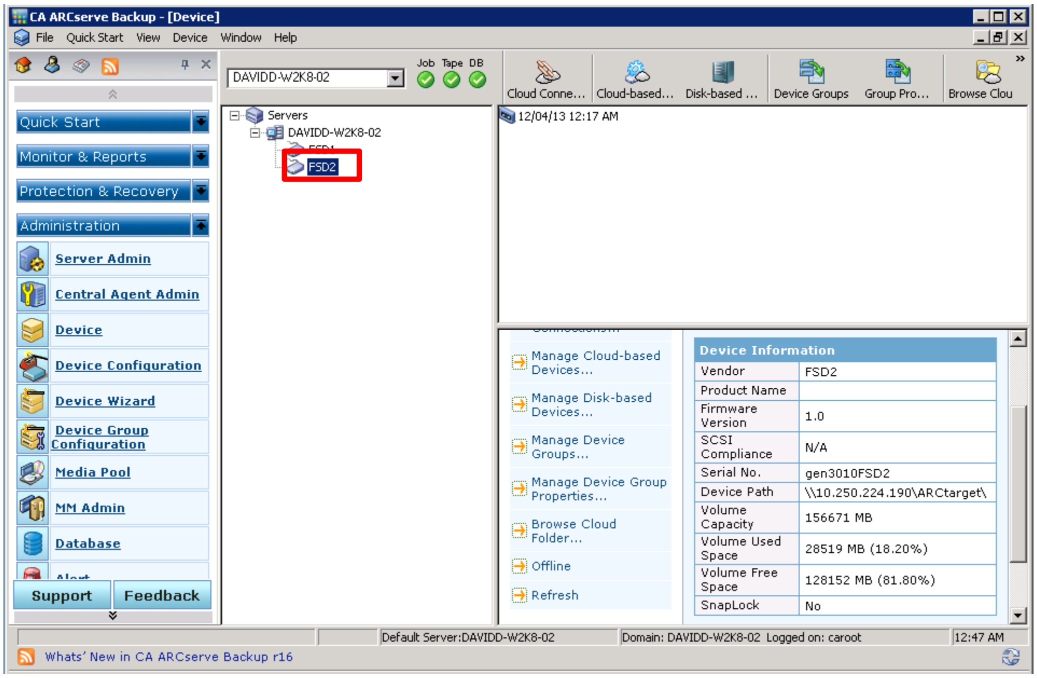
Number of Source Replications: 2

Local Container Name	Role	Remote Container Name	Peer State	Bandwidth	Select
ARCsource	source	10.250.224.190 ARCtarget	Online	Default	●
source	source	10.250.224.190 target	Online	Default	○

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

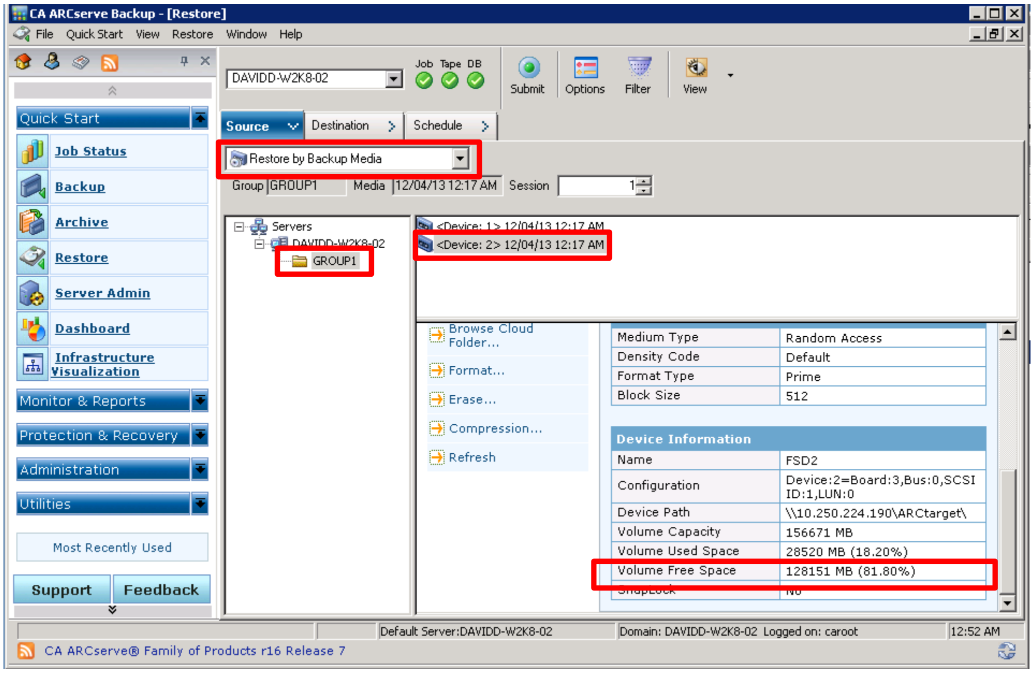
4.2 Restore from Replication Target

1. Restart ARCserve services. Go to **Administration** -> **Device**. Check and verify the target device.


CA ARCserve Backup - [Device]
File Quick Start View Device Window Help
DAVIDD-W2K8-02
Job Tape DB
Cloud Conne… Cloud-based… Disk-based … Device Groups Group Pro… Browse Clou
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
Support
Feedback
Servers
DAVIDD-W2K8-02
FSD1
FSD2
12/04/13 12:17 AM
Manage Cloud-based Devices…
Manage Disk-based Devices…
Manage Device Groups…
Manage Device Group Properties…
Browse Cloud Folder…
Offline
Refresh
Default Server:DAVIDD-W2K8-02
Domain: DAVIDD-W2K8-02 Logged on: caroot
12:47 AM
Whats' New in CA ARCserve Backup r16

Device Information	
Vendor	FSD2
Product Name	
Firmware Version	1.0
SCSI Compliance	N/A
Serial No.	gen3010FSD2
Device Path	\\10.250.224.190\ARCtarget\
Volume Capacity	156671 MB
Volume Used Space	28519 MB (18.20%)
Volume Free Space	128152 MB (81.80%)
SnapLock	No

2. Go to **Quick Start** -> **Restore**. Configure a restore job. Run the job to restore from the target device.



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

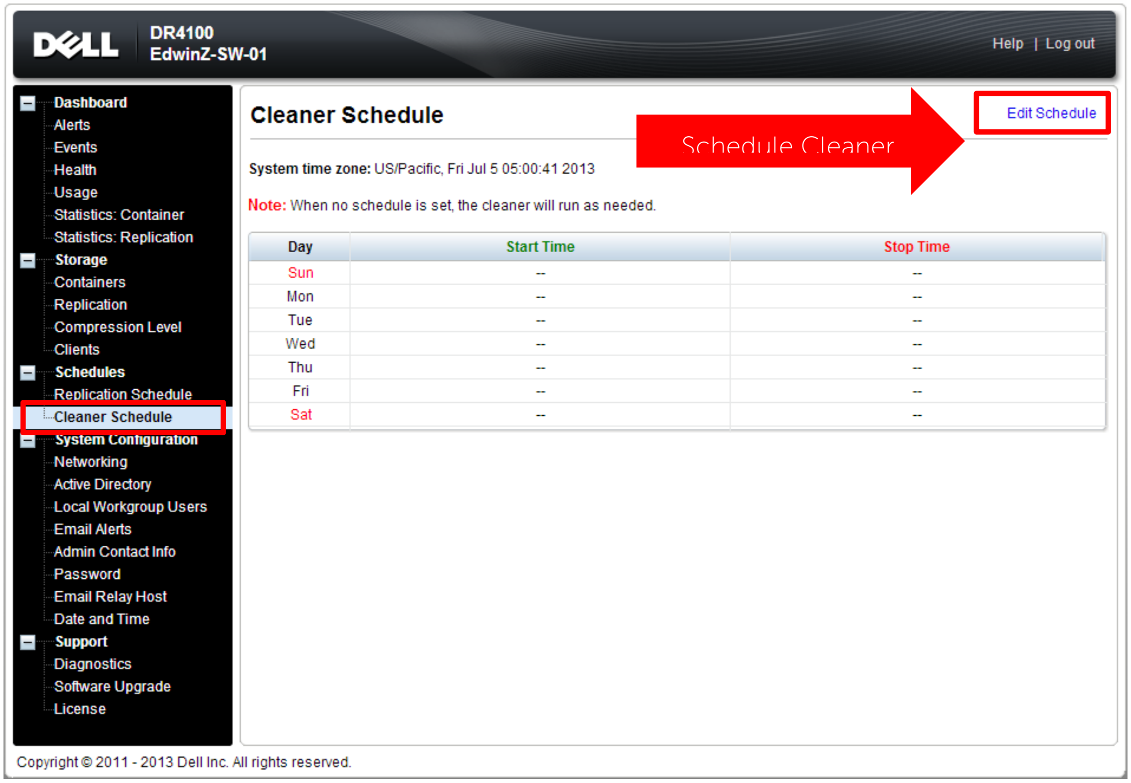
Device Information	
Name	FSD2
Configuration	Device:2=Board:3,Bus:0,SCSI ID:1,LUN:0
Device Path	\\10.250.224.190\ARCtarget\
Volume Capacity	156671 MB
Volume Used Space	28520 MB (18.20%)
Volume Free Space	128151 MB (81.80%)
SnapLock	No

5 Set Up the DR Series Deduplication Appliance Cleaner

The cleaner will run during idle time. If you 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 6 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.



Cleaner Schedule

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

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

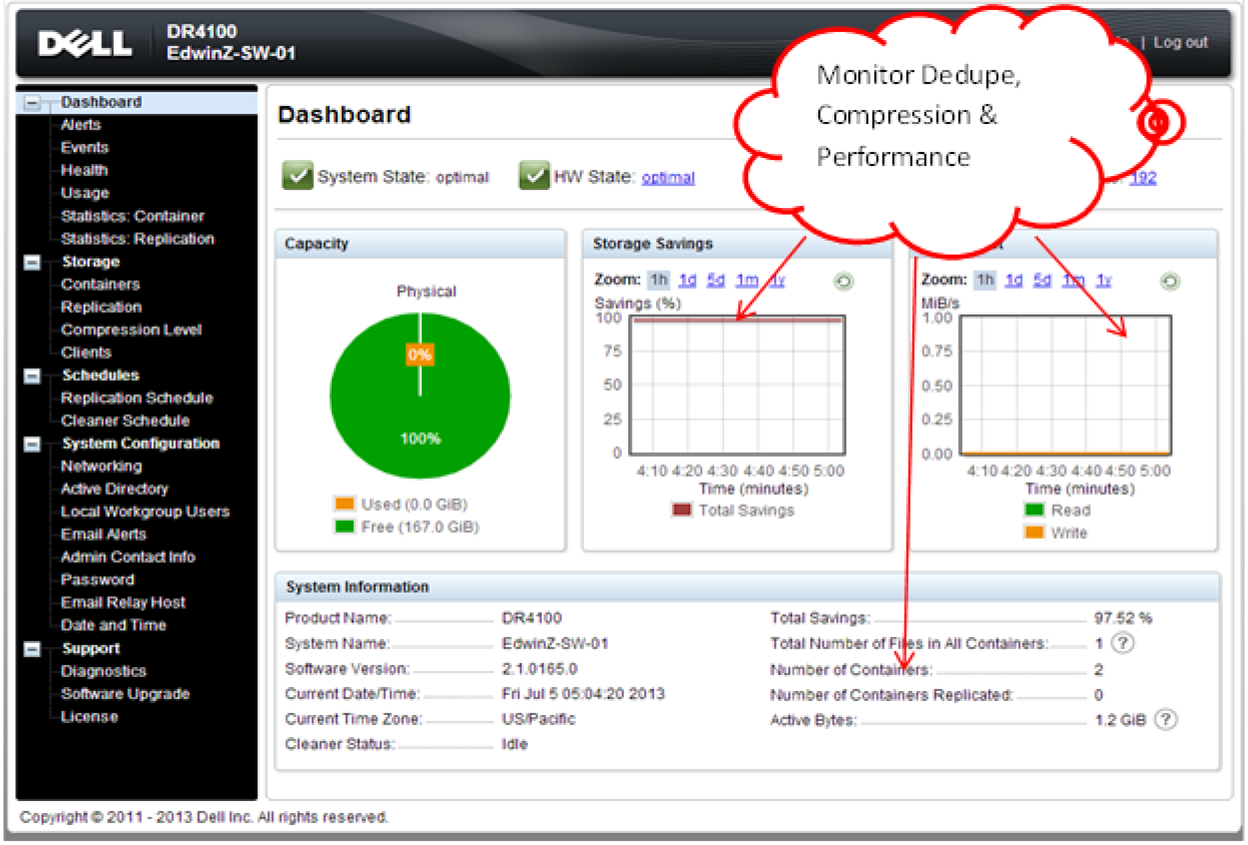
Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--

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

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 Deduplication Appliance.

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.



Monitor Dedupe, Compression & Performance

System State: optimal HW State: optimal

System Information

Product Name:	DR4100	Total Savings:	97.52 %
System Name:	EdwinZ-SW-01	Total Number of Files in All Containers:	1
Software Version:	2.1.0165.0	Number of Containers:	2
Current Date/Time:	Fri Jul 5 05:04:20 2013	Number of Containers Replicated:	0
Current Time Zone:	US/Pacific	Active Bytes:	1.2 GiB
Cleaner Status:	Idle		

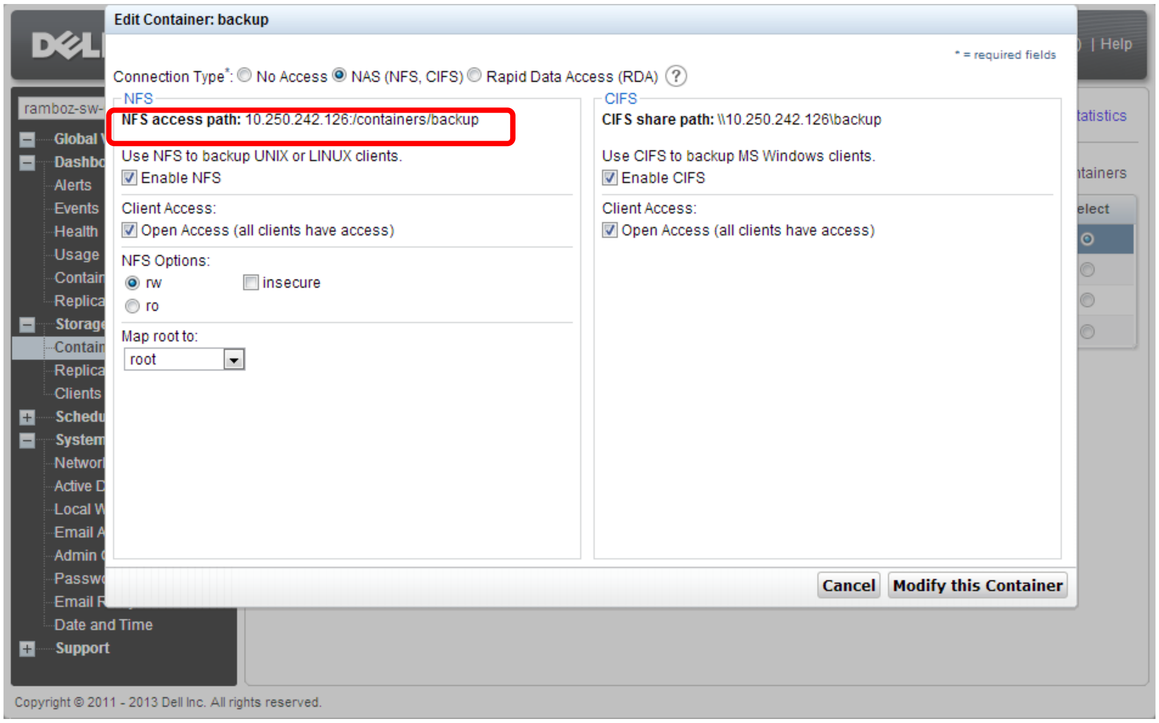
Copyright © 2011 - 2013 Dell Inc. All rights reserved.

A Appendix

A.1 Create a Storage Device for NFS

For NFS backup using the CA ARCserve, a target folder needs to be created as NFS share directory. This is the location to which backup objects will be written. This is not required while adding CIFS share.

1. Mount the DR Series Deduplication Appliance NFS share onto the NFS share directory which backup objects will be written in the CA ARCserve.
   Check the NFS access path:



Edit Container: backup

* = required fields

Connection Type*: ○ No Access ● NAS (NFS, CIFS) ○ Rapid Data Access (RDA)

NFS

NFS access path: 10.250.242.126:/containers/backup

Use NFS to backup UNIX or LINUX clients.

☑ Enable NFS

Client Access:

☑ Open Access (all clients have access)

NFS Options:

● rw ☐ insecure

○ ro

Map root to: root

CIFS

CIFS share path: \\10.250.242.126\backup

Use CIFS to backup MS Windows clients.

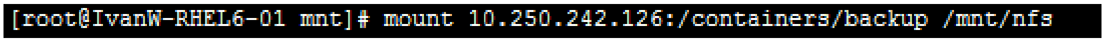
☑ Enable CIFS

Client Access:

☑ Open Access (all clients have access)

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

2. Mount NFS access path in Linux agent server
   Example:



```
[root@IvanW-RHEL6-01 mnt]# mount 10.250.242.126:/containers/backup /mnt/nfs
```