

Setting Up Quest® QoreStor™ with BridgeHead

## Technical White Paper

Quest Engineering

February 2023



## ALL RIGHTS RESERVED.

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

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED, OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

## Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

## Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Zmanda is a trademark of Zmanda Incorporated in the USA. All other trademarks and registered trademarks are property of their respective owners.

## Legend



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



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



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

Setting Up Quest® QoreStor™ with BridgeHead

Updated – February 16, 2023

# Contents

1. Installing and configuring QoreStor.....	5
2. Creating a CIFS container for use with BridgeHead .....	6
3. Adding QoreStor CIFS container to BridgeHead .....	8
4. Create a New Backup Job with QoreStor CIFS container as the Target .....	10
5. Setting up the QoreStor system replication .....	30
Creating a CIFS/NFS replication session.....	30
6. Restoring from the replication target .....	32
7. Creating RDS container for use with BridgeHead:.....	35
8. Add RDS container to Bridgehead .....	38
9. Setting up Cloud Tier .....	64
Creating a policy driven Cloud Tier.....	64
8. Cloud Reader.....	69
9. Performance Tier .....	76
Setting up Performance Tier with QoreStor .....	76
10. Setting up the QoreStor system cleaner .....	79
11. Monitoring deduplication, compression and performance.....	81
Appendix .....	82
A. Create a Storage Device for CIFS .....	82
B. Create a Storage Device for NFS .....	84

# Executive Summary

This paper provides information about how to set up Quest® QoreStor™ as a backup target for BridgeHead Backup software.

For additional information, see the QoreStor documentation and other data management application best practices whitepapers for your specific QoreStor version at:

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

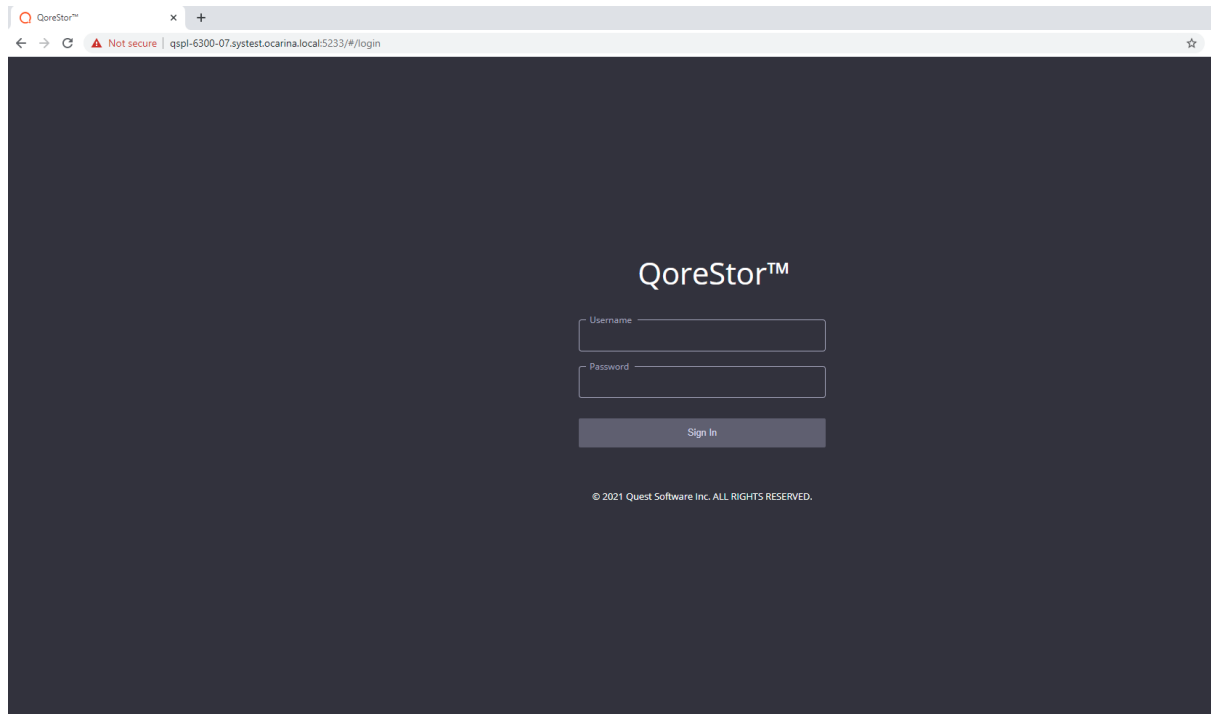
**i** | **NOTE:** The QoreStor and BridgeHead screenshots used in this document may vary slightly, depending on the QoreStor and BridgeHead versions you are using.



# 1. Installing and configuring QoreStor

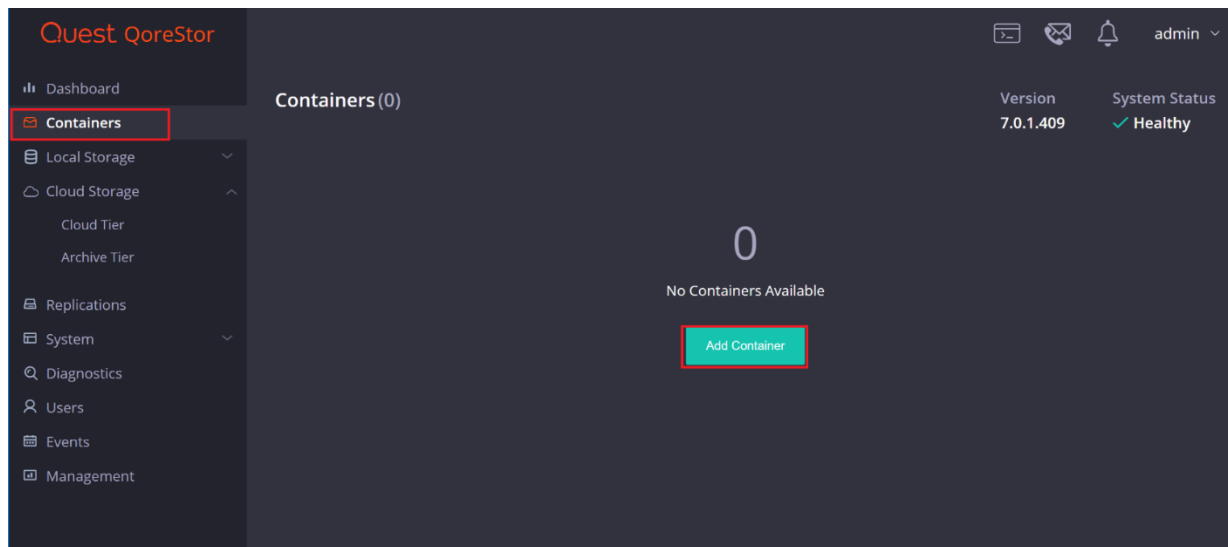
- 1 Before installing QoreStor, refer to the *QoreStor Interoperability Guide* to ensure your system(s) meet the installation requirements.
- 2 To install QoreStor on your system(s), follow the procedures documented in the *QoreStor Installation Guide*.

Using a supported web browser (refer to *QoreStor Interoperability Guide* for a list of supported browsers), connect to the QoreStor administrative console via https, using the host IP address/FQDN and port 5233 (https://<hostname:5233>). Log in with the username `admin` and password `st0r@ge!` (The “0” in the password is the numeral zero).



## 2. Creating a CIFS container for use with BridgeHead

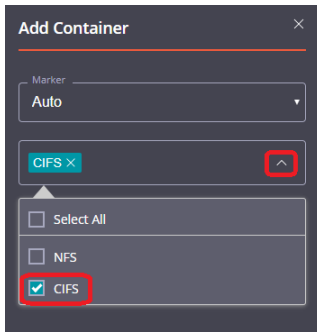
- 1 Select the **Containers** tab, then click **Add container**.



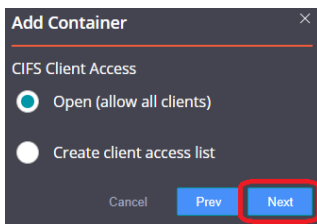
- 2 Enter a container **Name**, select a **Storage Group** or leave the **DefaultGroup** option selected, and select **NAS (NFS, CIFS)** from the **Protocol** dropdown menu. Click **Next**.

The screenshot shows a 'Add Container' dialog box with a close button (X) in the top right corner. It contains three input fields, each with a red border: a text field for 'Name', a dropdown menu for 'Storage Group' with 'DefaultGroup' selected, and a dropdown menu for 'Protocol' with 'NAS (NFS, CIFS)' selected. At the bottom, there are three buttons: 'Cancel', 'Prev', and 'Next', with the 'Next' button highlighted by a red box.

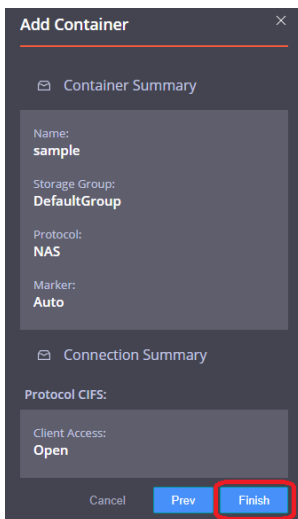
- 3 Click the dropdown on the **Protocols** field then select the check mark for **CIFS**. Leave **Marker Type** on **Auto**, then click **Next**.



- 4 Fill in the **CIFS Client Access** options if needed then click **Next**.

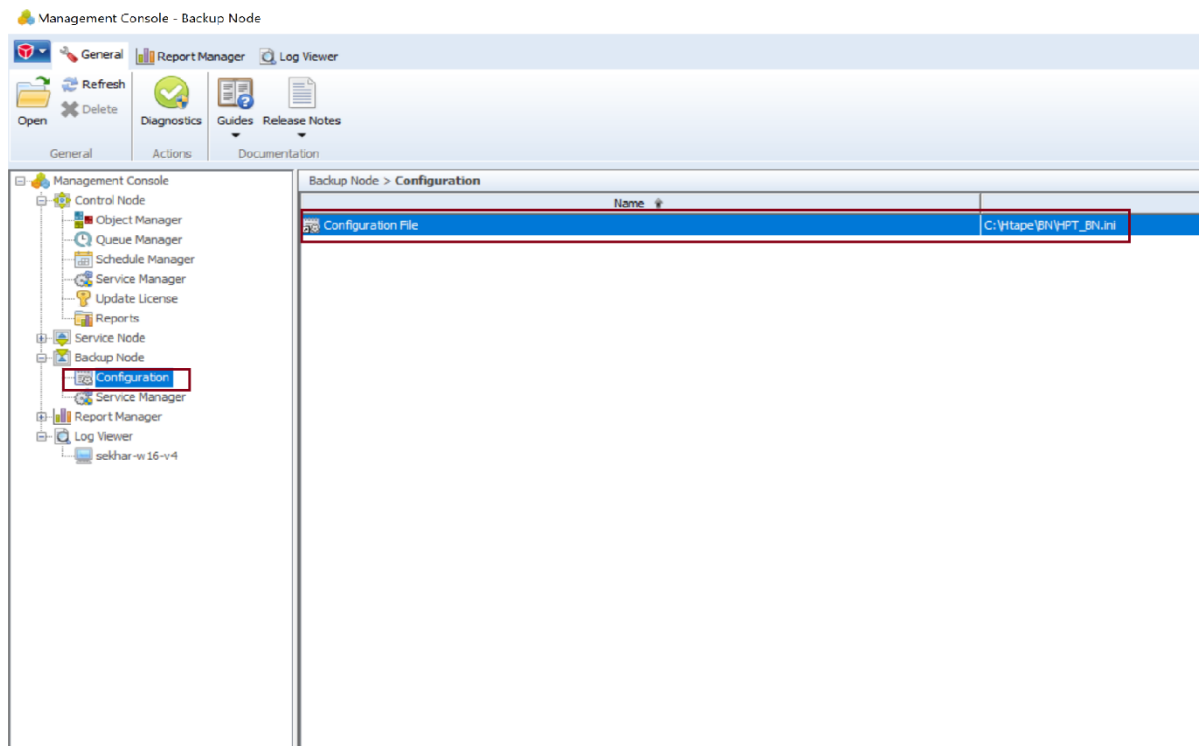


- 5 Confirm the settings and click **Finish**. Confirm that the container is added.



### 3. Adding QoreStor CIFS container to BridgeHead

- 1 Open BridgeHead Console Management console.
- 2 Under **Backup Node**, click **Configuration**. Double-click to open the Configuration File.



- 3 Search **Staging\_Area** in the text editor. Use QoreStor container share UNC path for the **Staging Area Path**, define a **Staging Area Name**. Save the Configuration file.

```
HPT_BN - Notepad
File Edit Format View Help

; the staging area size is limited only by the amount of free disk
; space available.
;
;
; Staging_Area<_nn>_Path
; Specifies the full path of the staging area. For example
; C:\Stage\Stage1\. The default is no path, i.e. no staging area.
; Staging areas have to be defined in strict ascending order.
; For example if one defines staging areas 01, 02, 03, 05, 06 and 07,
; only staging areas 01, 02 and 03 will be taken into account.
; If not defined, Staging_Area_01_Path defaults to the Stage
; sub-folder of the Backup Node. Typically C:\Htape\BN\Stage.
;
Staging_Area_01_Path = \\10.230.48.240\sample
Staging_Area_02_Path = C:\Stage\Stage2\
;
; Staging_Area<_nn>_Name
; Specifies a name for the staging area. This setting is optional.
; If you specify a staging area name, you can ask the Backup Node to
; select that particular staging area, rather than leave the choice
; to the Backup Node. The default is no name.
;
Staging Area 01 Name = HDMCIFS
Staging_Area_02_Name = Stage2
;
; Staging_Area<_nn>_Max_Size
; Specifies the maximum size of the staging area, in MB. This setting
<
```

**Note:** The Backup Node for BridgeHead Healthcare Data Management requires appropriate permissionsto the QoreStor CIFS Share for the step below to complete successfully. See **Appendix A** for setting up the BridgeHead Healthcare Data Management Backup Node account correctly.This should be done before the next step.

## 2.1 Procedure for Unix/Linux Environment

### Notes:

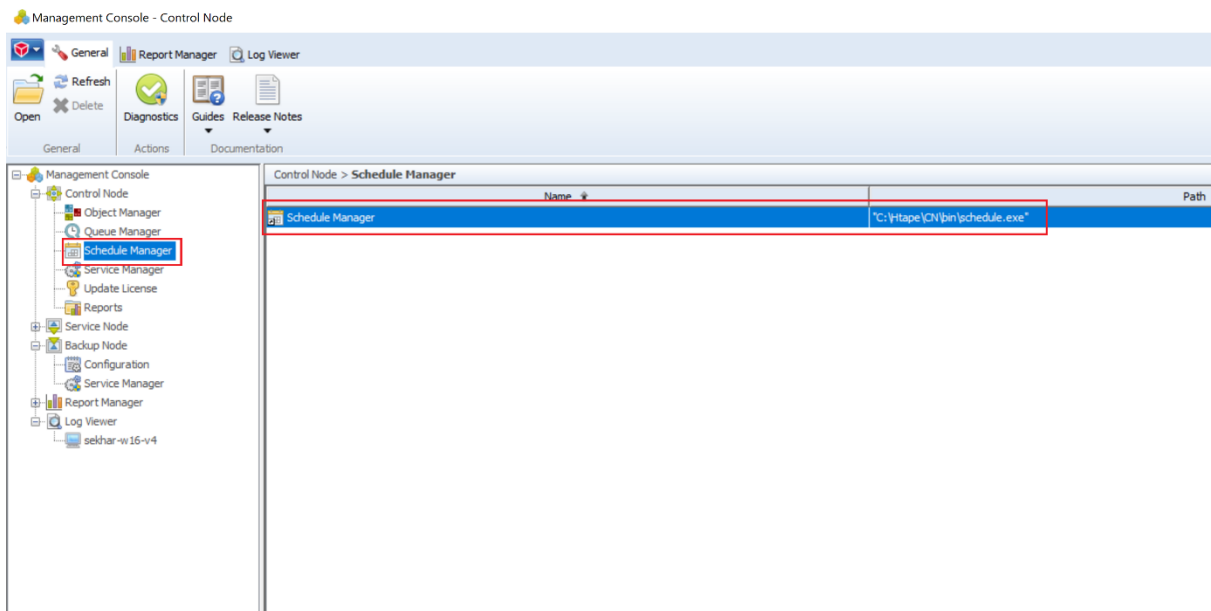
Make sure that you can mount/verify the NFS share from the UNIX/Linux backup node. Please see **Appendix B** for how to mount/verify the NFS share.

The procedure for the Unix/Linux Environment is very similar to the procedure for the Windows Environment. One difference is that the configuration file of the Backup Node is **ht\_media.def**, and the default location for the file is **“/etc/ht\_media.def”**.

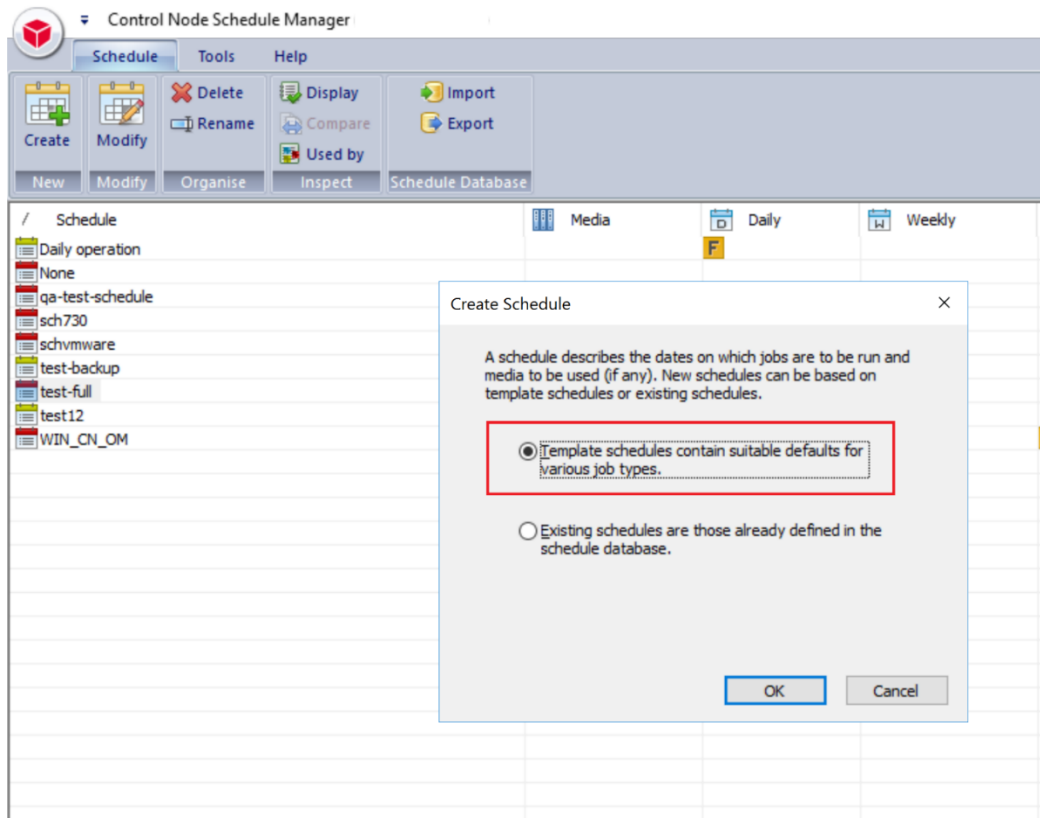
For other details, please refer to the Procedure for the Windows Environment.

## 4. Create a New Backup Job with QoreStor CIFS container as the Target

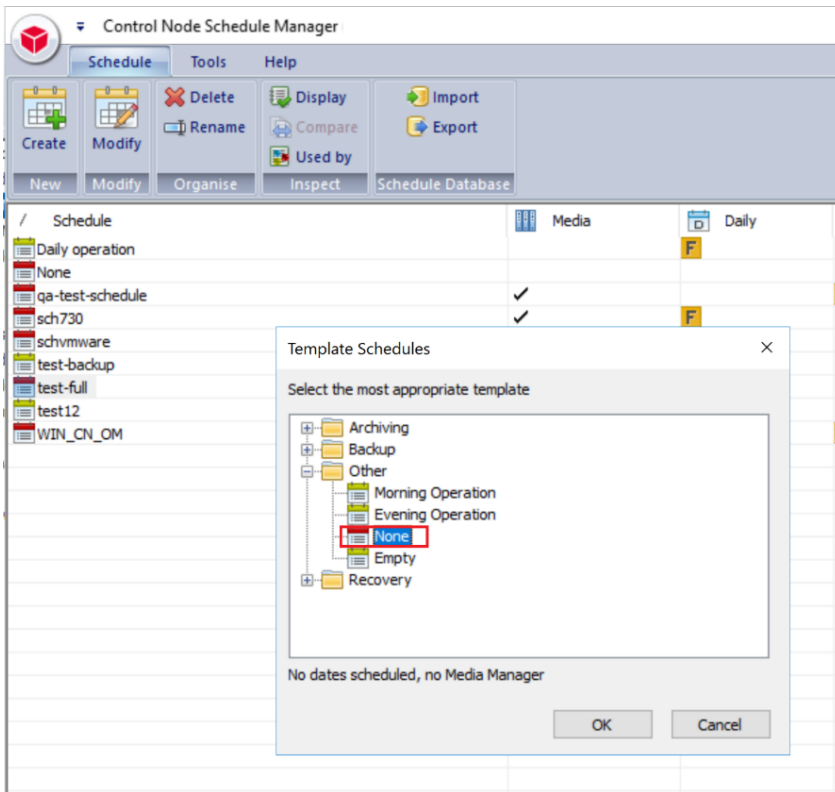
1. Open **BridgeHead Management Console**. Click **Schedule Manage** under **Control Node**. Double-click to open the **Schedule Manager**.



2. Select Template schedules that contain suitable defaults for various job types. Click **OK**.

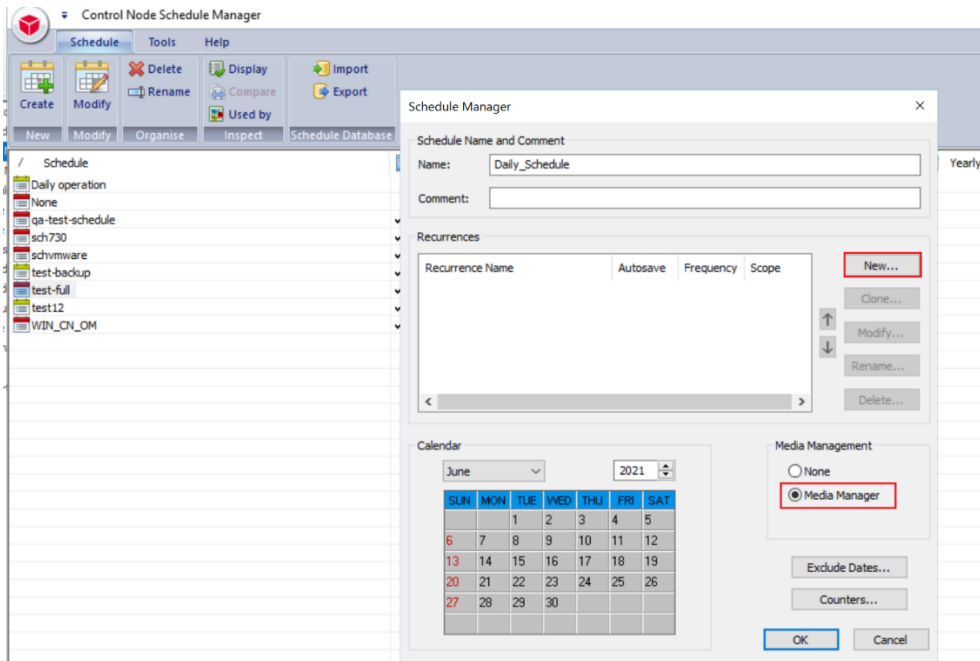


3. Select None and then click **OK**.

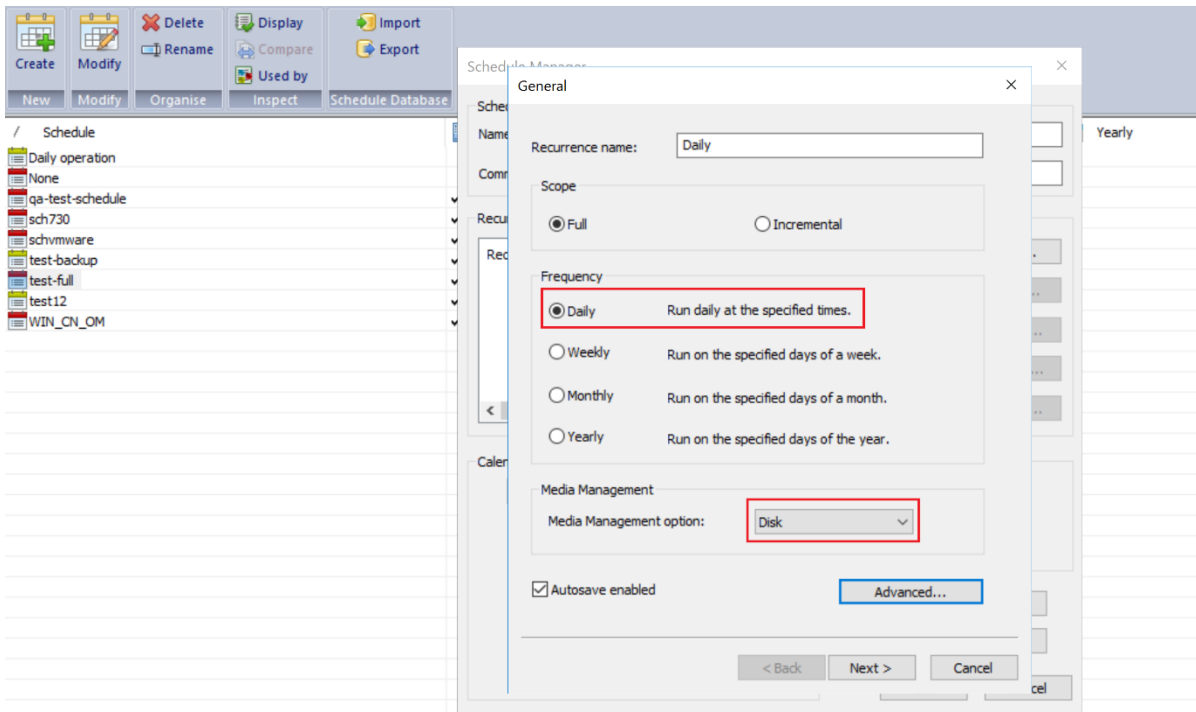




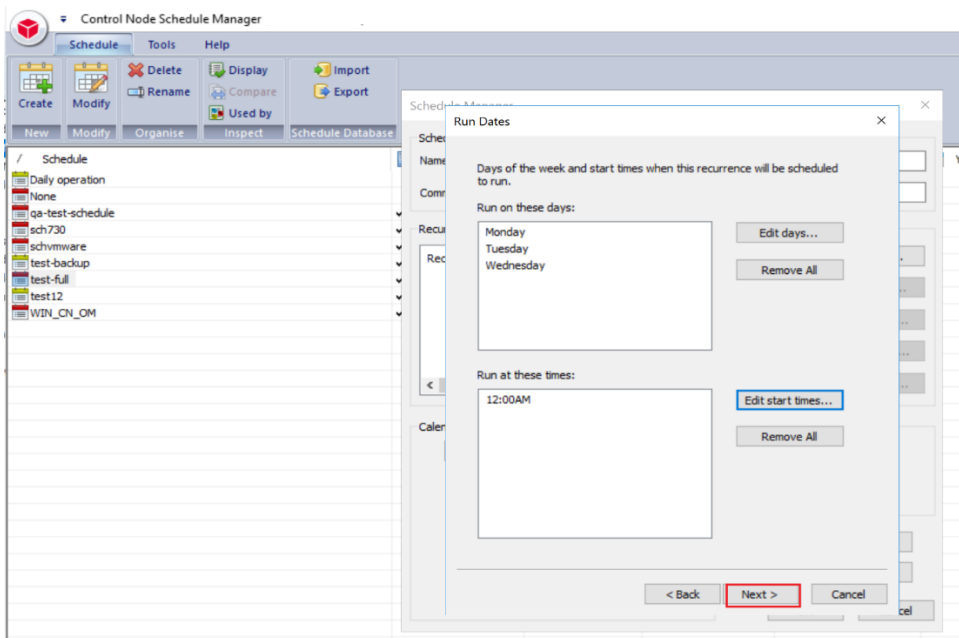
4. Populate all the required fields and SelectMedia Manager under Media Management, and click **New**.



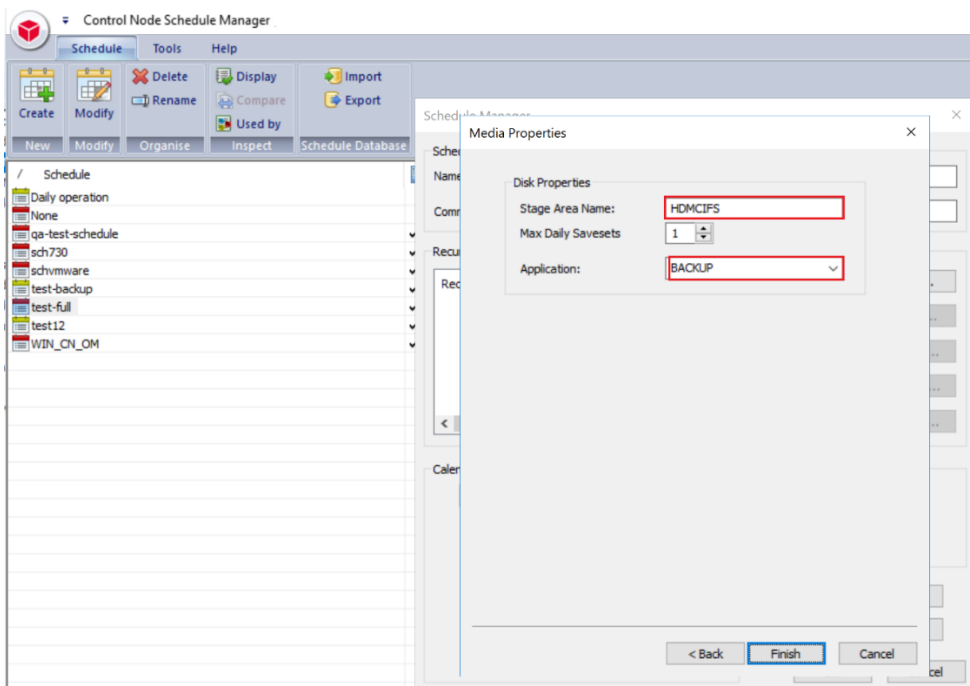
5. Select Disk in the Media Management option and click **Next**.



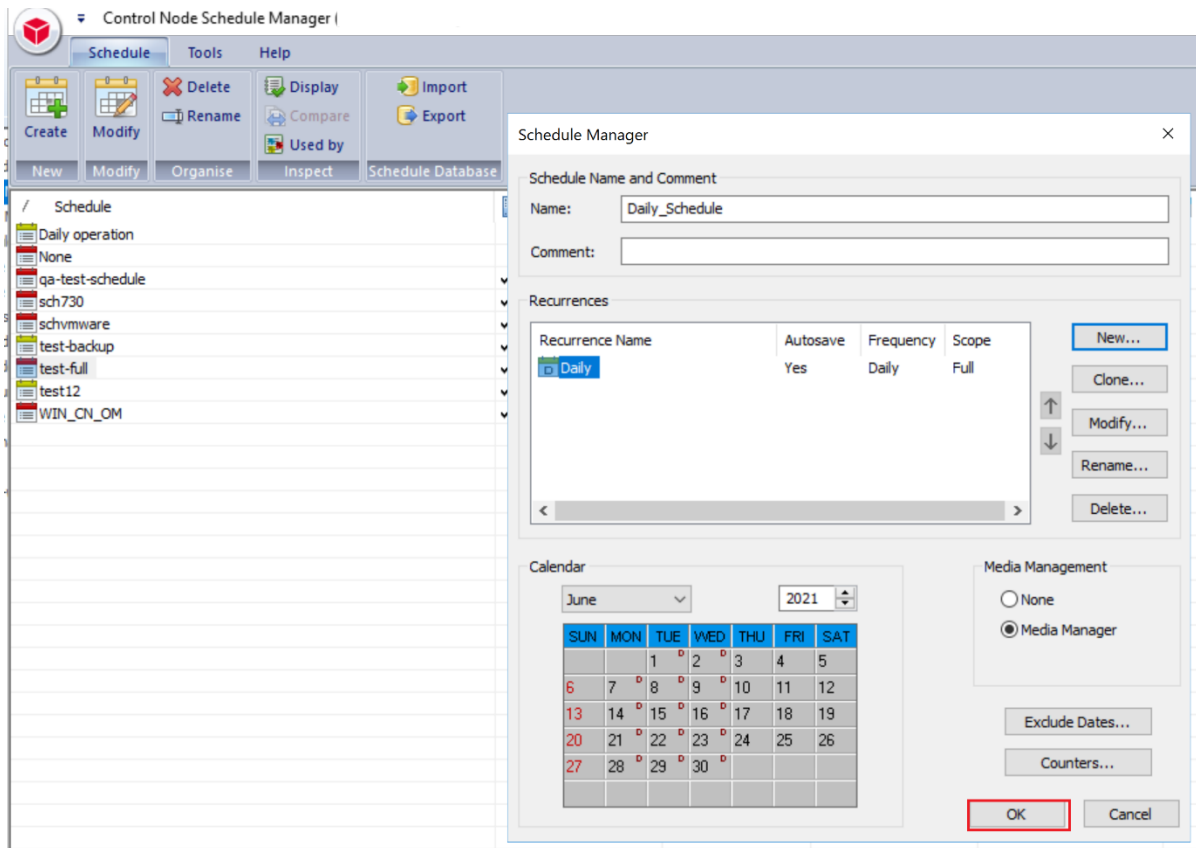
6. Select all the required fields then click NEXT



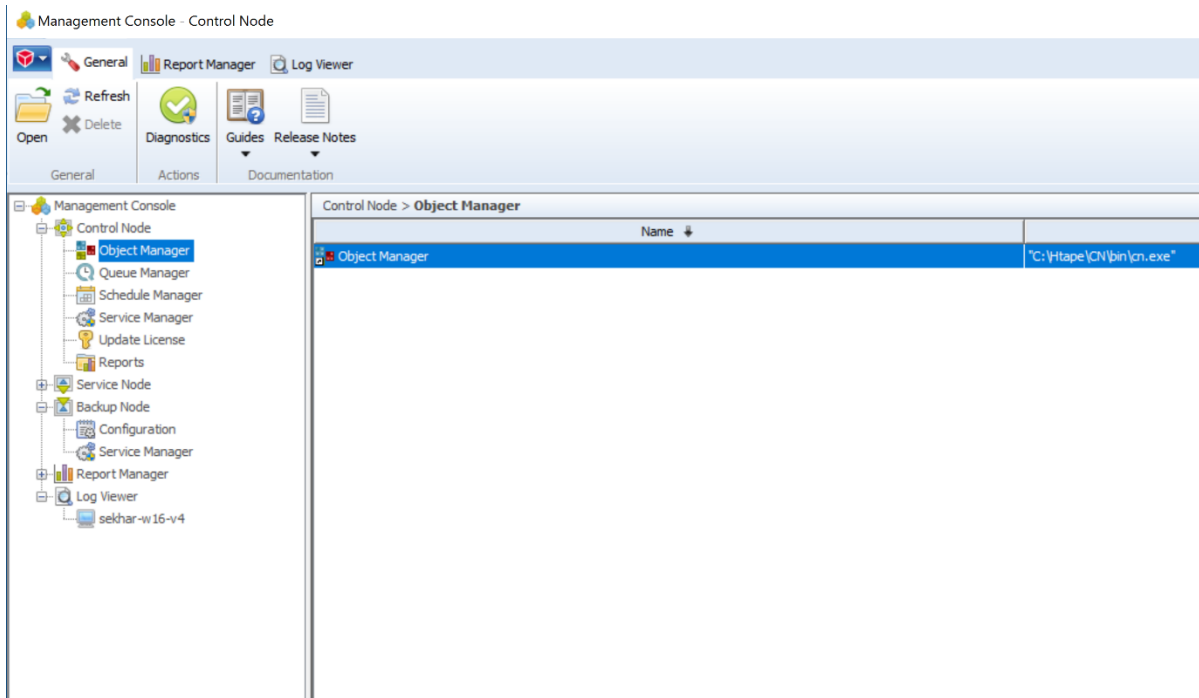
7. Enter Stage Area Name, Application as BACKUP, click **Finish**.



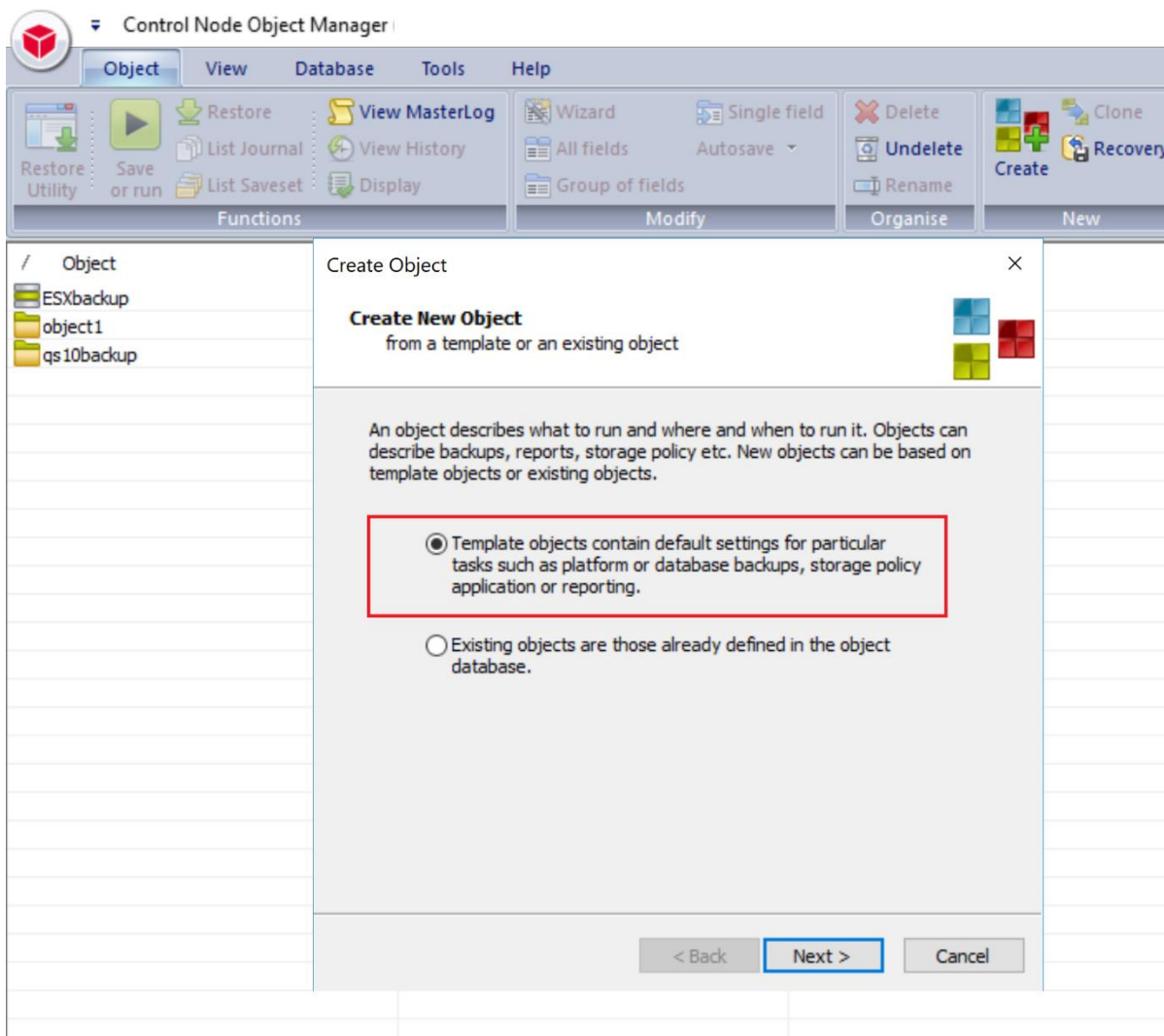
8. Click OK to save it.



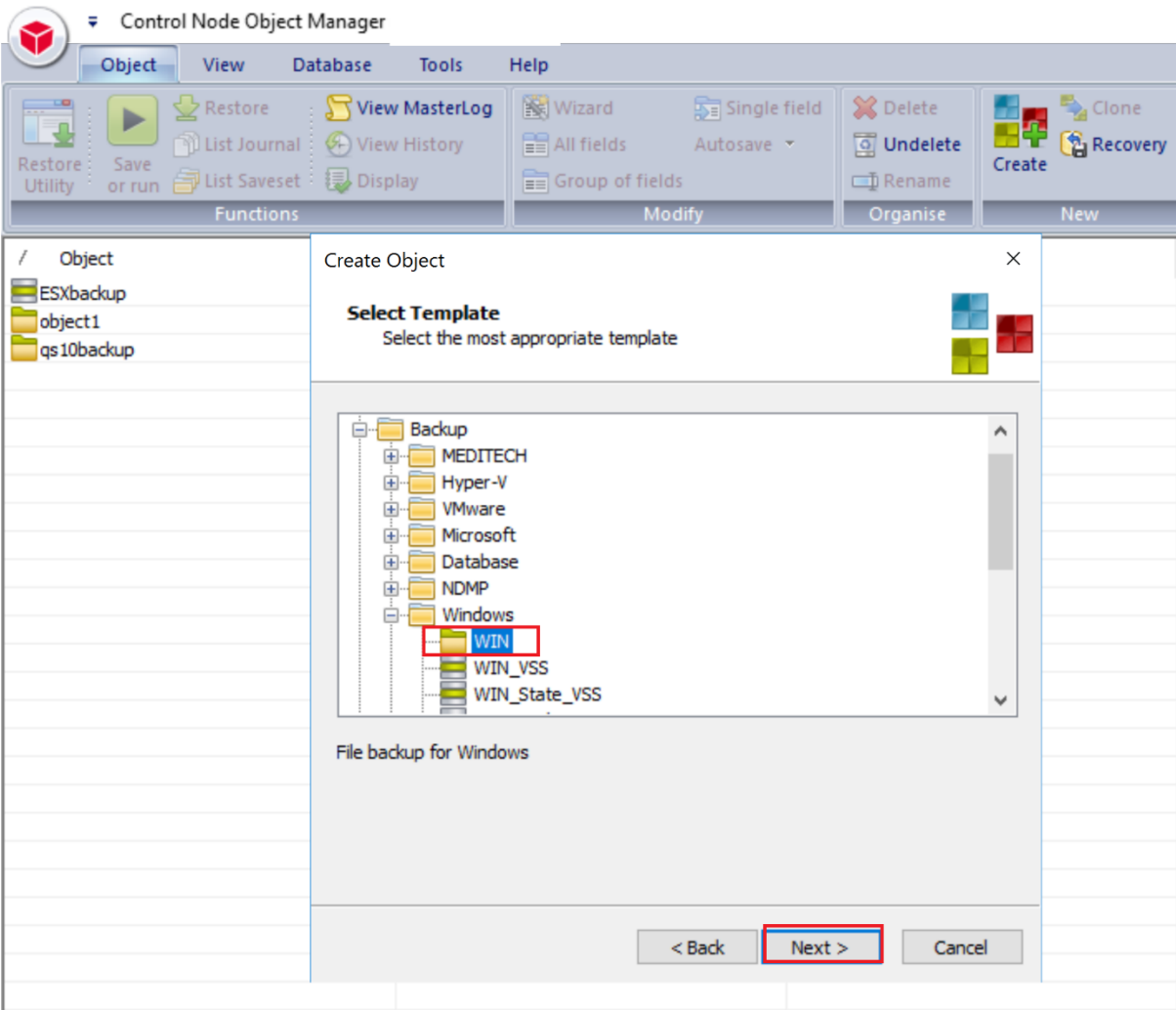
9. On Bridge HDM Management Console, click Object Manager under Control Node, which displays the Object Manager in the list. Double-click to open the Object Manager on right- hand side pane.



10. Select the **Template objects** to contain default settings for particular tasks such as platform or database backups, storage policy applications, or reporting, and click **Next**.



11. Select **WIN** in the template list then click **Next**.



12. Enter the **Service Node** related info with the valid file path for the backup data source, click on Credential manager to set the password and then click **Next**.

The screenshot shows the 'Control Node Object Manager' application. The 'Object' menu is selected, and the 'Create Object' dialog is open. The dialog is titled 'Create Object' and has a close button (X) in the top right corner. The 'Service Node' tab is selected, indicated by a blue square icon. Below the title, there is a description: 'A Service Node is a computer whose data is saved or restored by an operation initiated a Control Node. During a save, data is collected and sent to a Backup Node.' The dialog contains three main input fields, each highlighted with a red rectangle: 'Computer:' with a dropdown menu showing 'localhost', 'Credential:' with a dropdown menu showing 'administrator', and 'Path:' with a text box containing 'C:\dataset'. There is a 'Credential Manager...' button next to the 'Credential:' field. At the bottom of the dialog, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The background application window shows a menu bar with 'Object', 'View', 'Database', 'Tools', and 'Help'. The 'Object' menu is open, showing options like 'Restore Utility', 'Save or run', 'List Journal', 'List Saveset', 'View MasterLog', 'View History', 'Display', 'Wizard', 'All fields', 'Group of fields', 'Single field', 'Autosave', 'Delete', 'Undelete', 'Rename', 'Clone', 'Recovery', and 'Create'.

Control Node Object Manager

Object View Database Tools Help

Restore Utility Save or run List Journal List Saveset View MasterLog View History Display Wizard All fields Group of fields Single field Autosave Delete Undelete Rename Clone Recovery Create

Functions Modify Organise New

/ Object

- ESXbackup
- object1
- qs10backup

Create Object

**Service Node**

A Service Node is a computer whose data is saved or restored by an operation initiated a Control Node. During a save, data is collected and sent to a Backup Node.

Computer: localhost

Credential: administrator

Credential Manager...

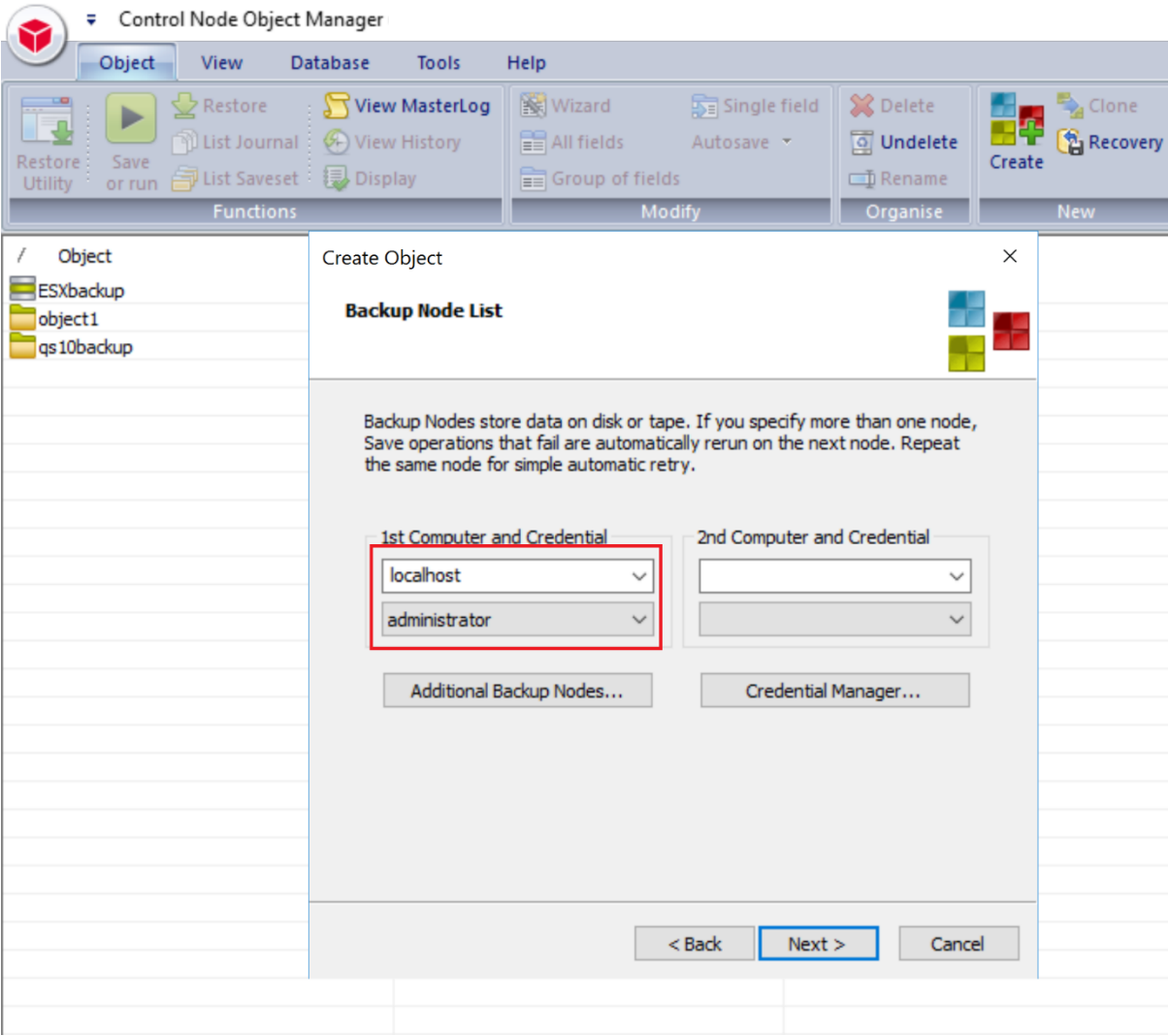
Path defines data to be saved or restored

Path: C:\dataset

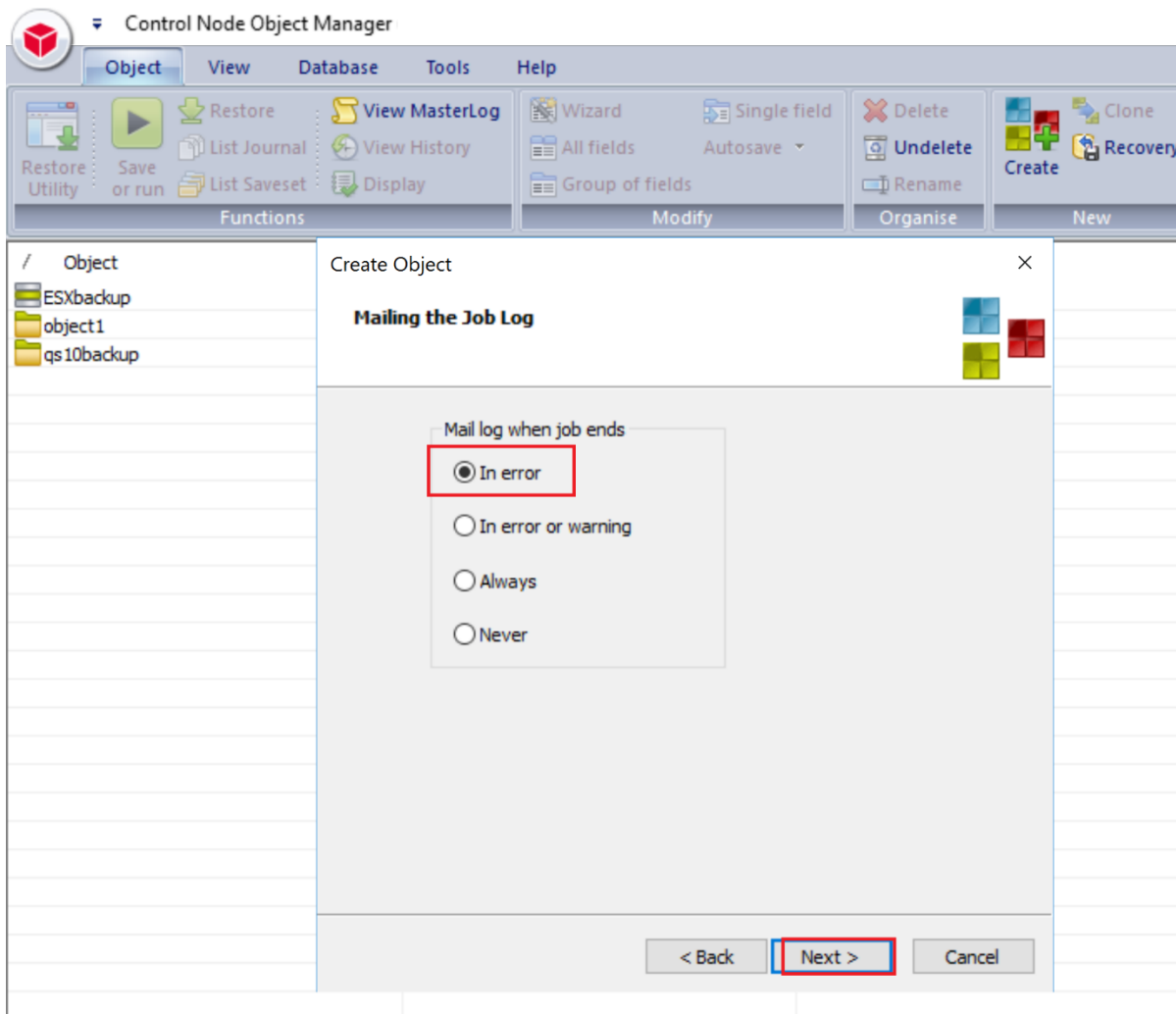
< Back Next > Cancel



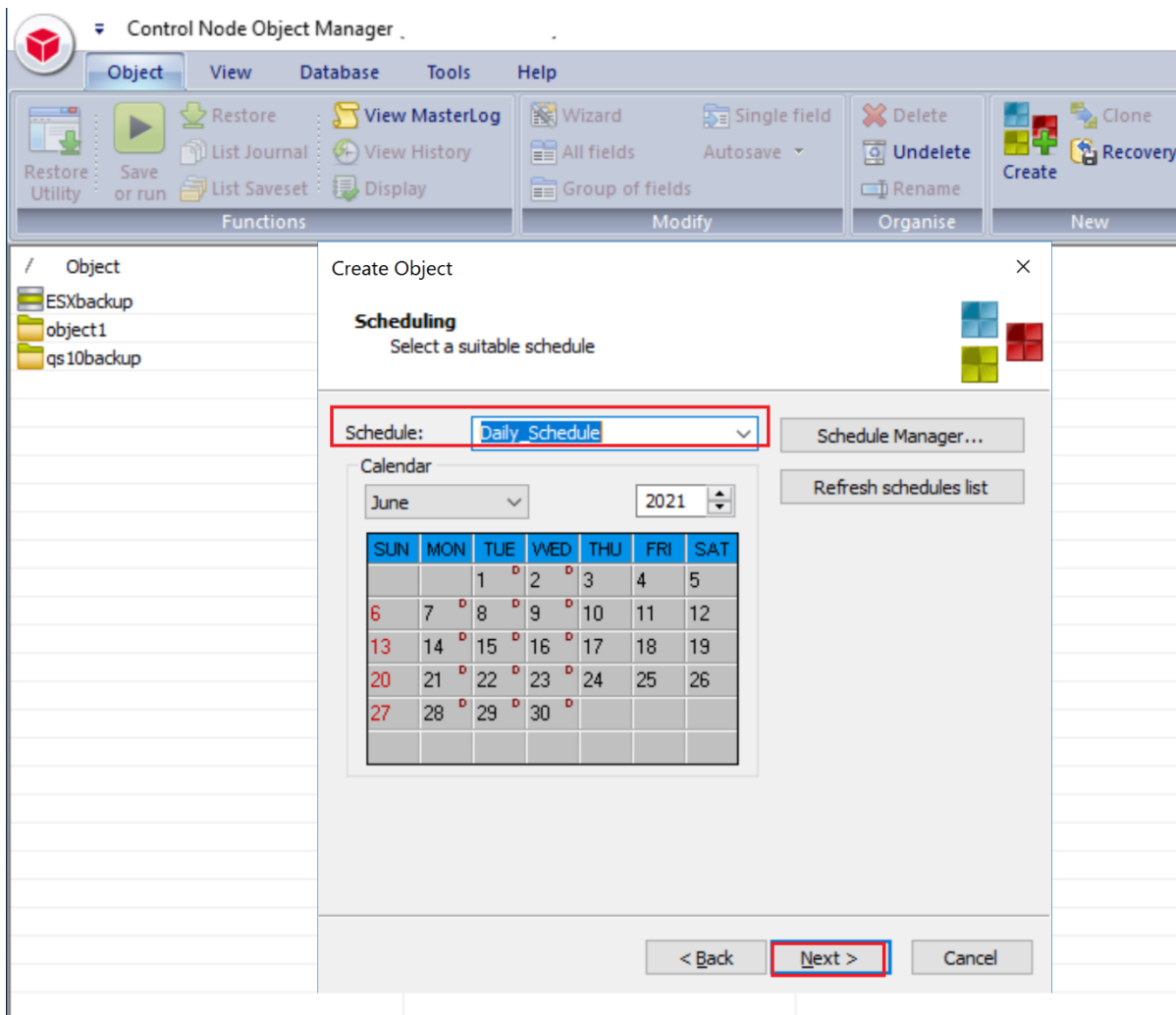
13. Enter **Backup Node** related info.



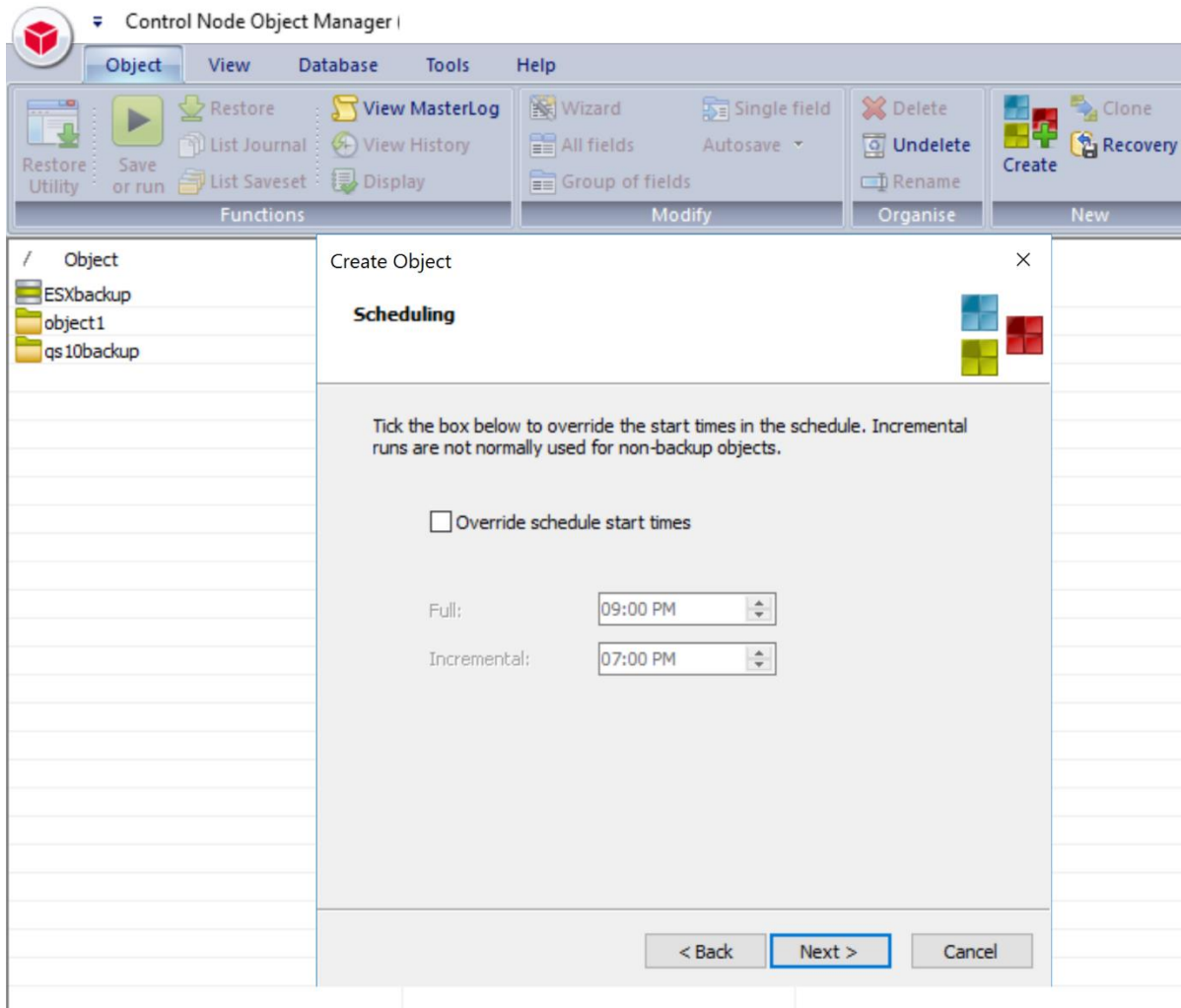
14. Accept the defaults and click **NEXT**.



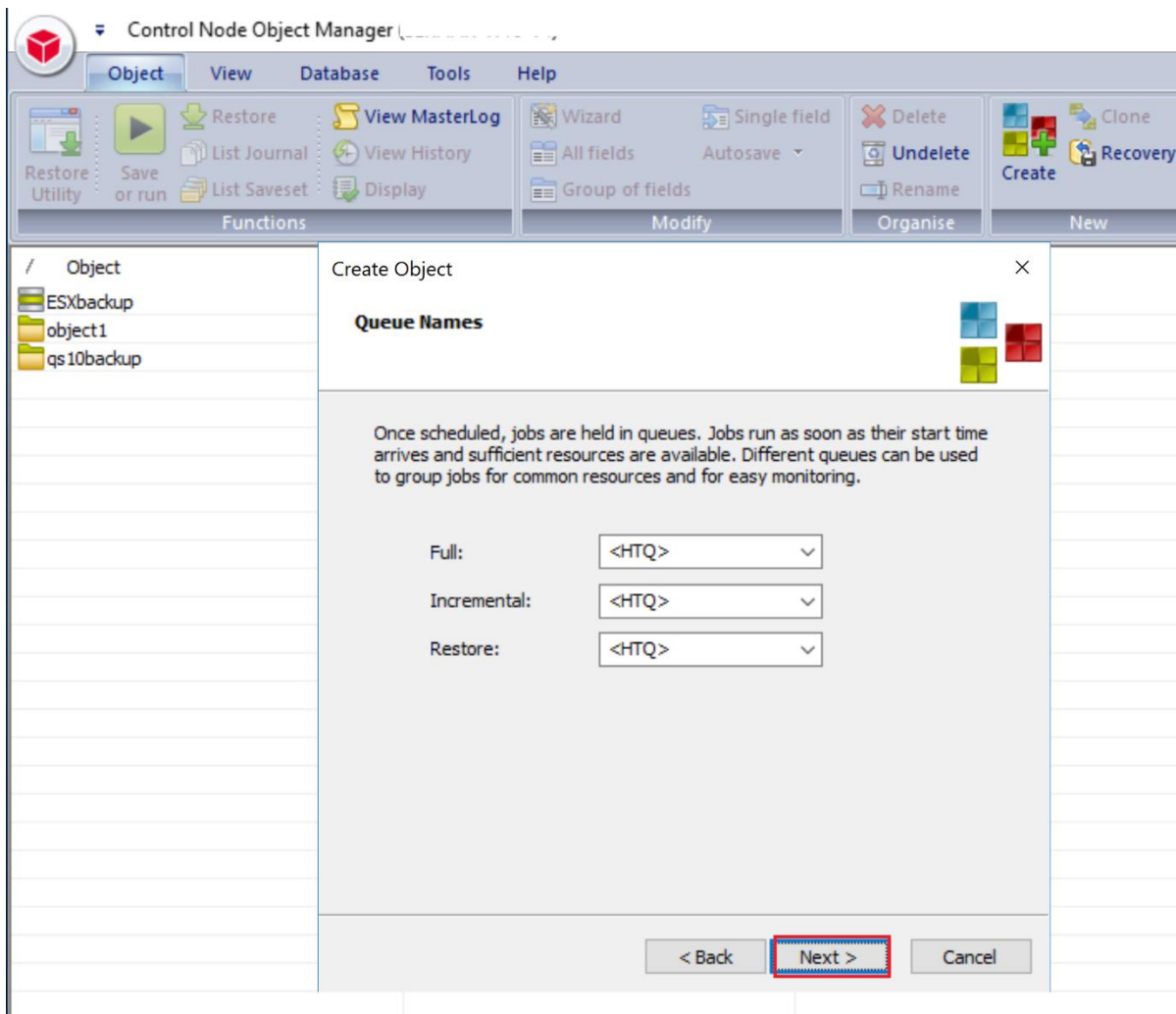
15. Select the schedule, and click **NEXT**.



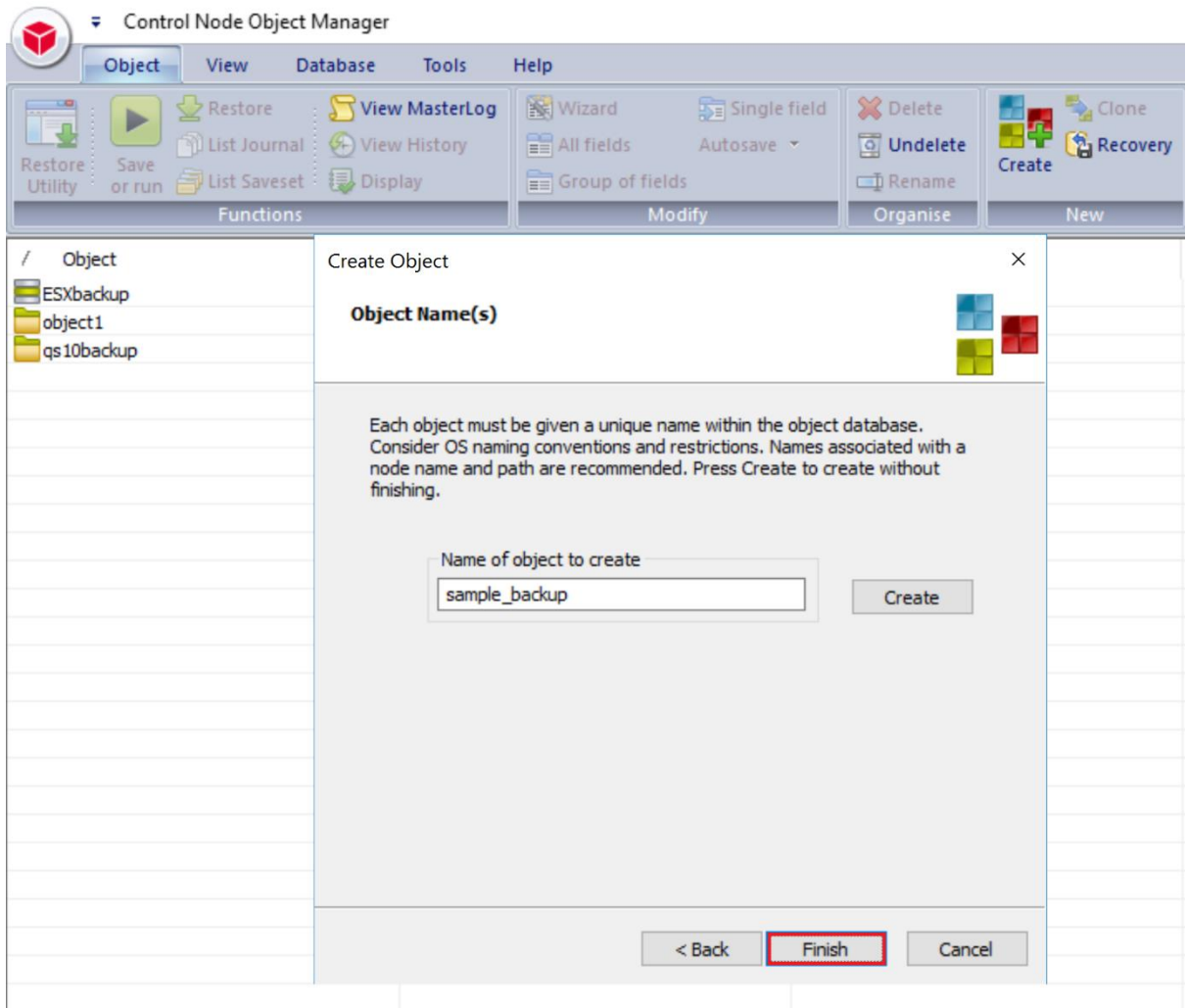
16. Accept the defaults and click **Next**.



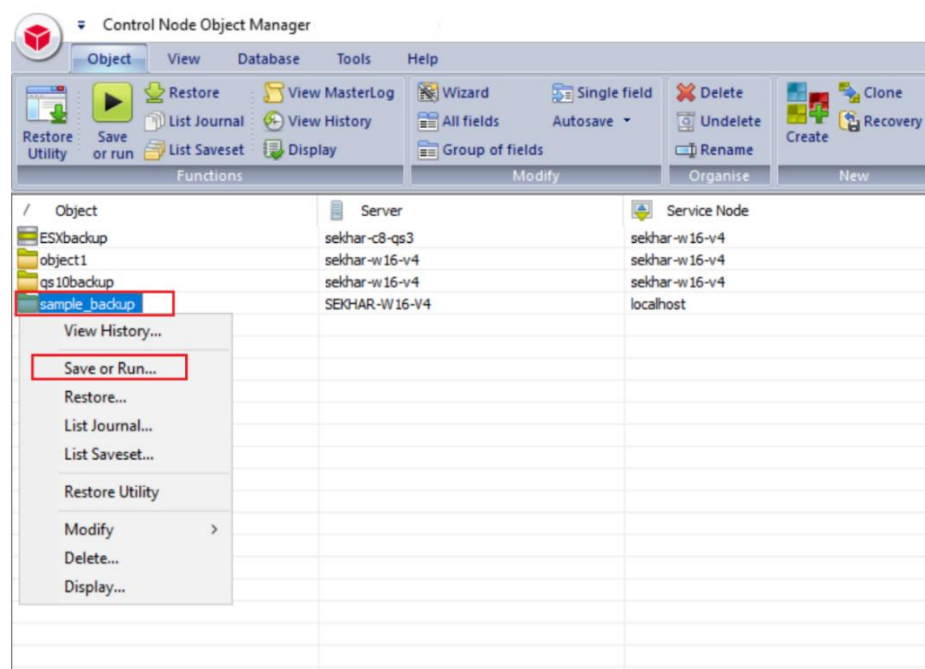
17. Accept the defaults and click **Next**.



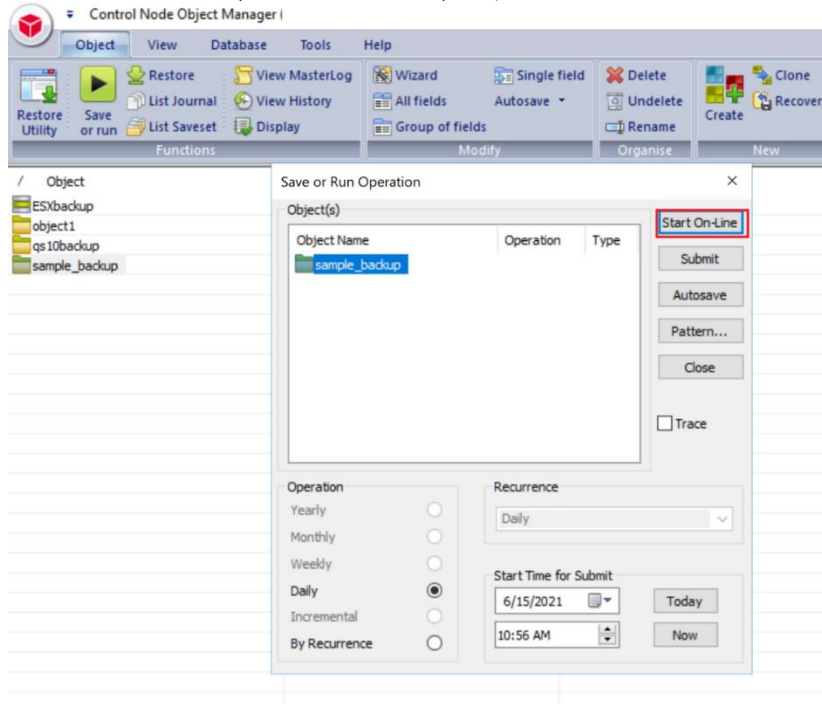
18. Enter the Name of the Object then click **Finish** to save it.



19. The backup object summary is displayed on the Object list. Right-click the object to run the backup.

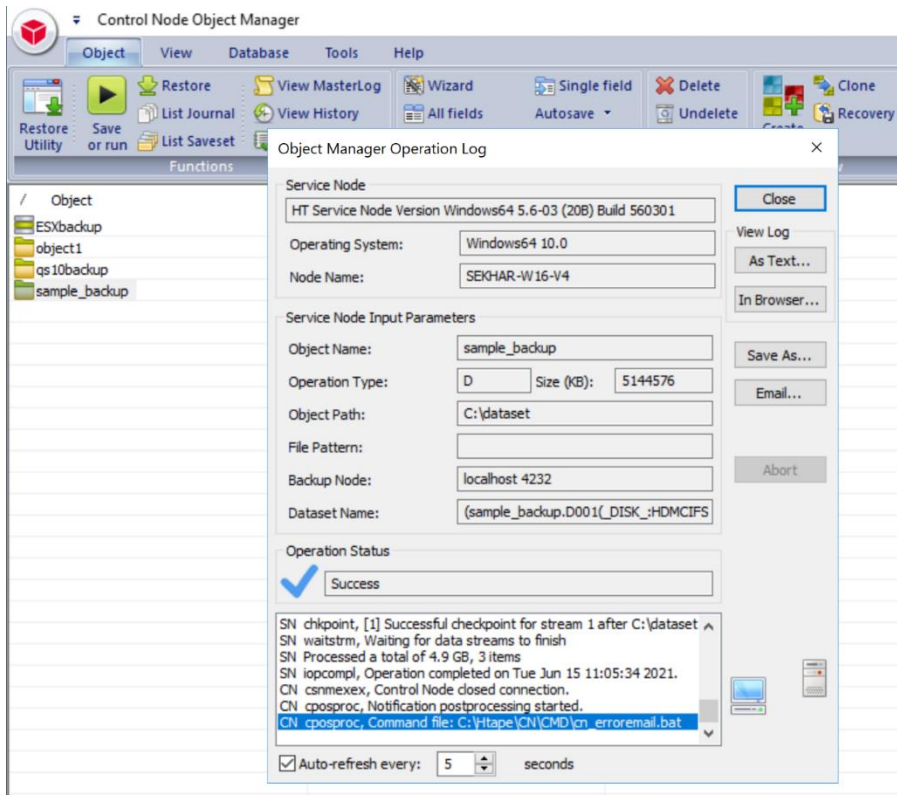


20. When Save or Run Operation window opens, click Start On-Line to start the backup.





21. The Object Manager Operation Log window displays the progress of the backup session. Operation status has details of the backup job.

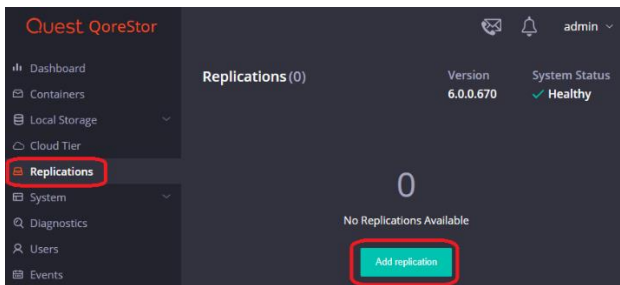


## 5. Setting up the QoreStor system replication

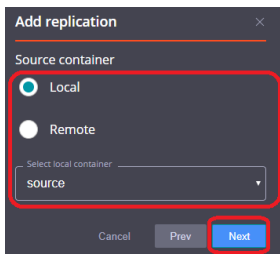
**i** **NOTE:** For the steps in this procedure, assume QS1 is the replication source QoreStor system, and QS2 is the replication target QoreStor system. 'source' is the replication source container, and 'target' is the replication target container.

### Creating a CIFS/NFS replication session

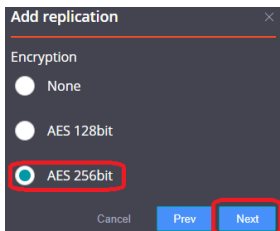
- 1 Create a source container on the source QoreStor system.
- 2 Create a target container on the target QoreStor system.
- 3 On the source QoreStor system, go to the **Replications** Tab. Click the **Add replication** button.



- 4 Select the source Container for Replication and click **Next**.



- 5 Select the **Encryption** type for the Source Container and click **Next**.



- 6 Enter the target QoreStor systems related information then click **Retrieve Remote Containers**. Select a target container from the populated list, and click **Next**.

Add replication

Target container

☐ Local

☒ Remote

Username  
admin

Password  
\*\*\*\*\*

Remote Machine  
qspl6300-47.systest.ocarina.local

Retrieve Containers

Select remote container  
target

Cancel Prev Next

- 7 Specify any **Bandwidth Limitations** needed in MBps, and leave 0 for unlimited bandwidth. Click **Next**.

Add replication

Limits

Bandwidth Limit for the peer machine [Mbps]  
0

Cancel Prev Next

- 8 Verify the Summary and click **Finish**.

Add replication

Source container

Source  
Local

Container  
source

Encryption

Algorithm  
AES 256

Limits

Bandwidth Limit [Mbps]  
Unlimited

Target

Source  
Remote

Container  
target

User  
admin

Password  
\*\*\*\*\*

Remote Machine Address  
qspl-6300-47.systest.ocarina.local

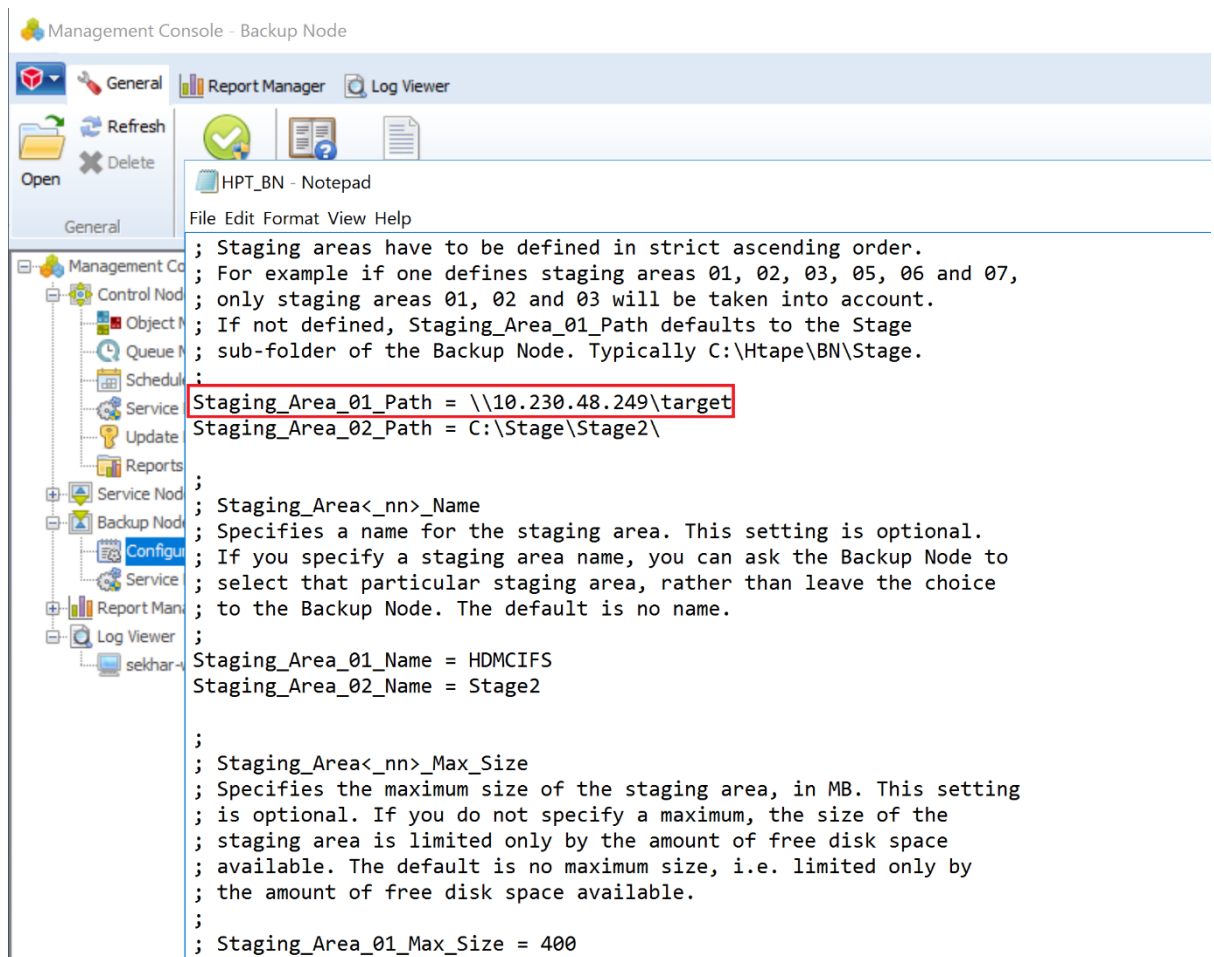
Cancel Prev Finish

- 9 Check replication is added successfully and confirm the replication details

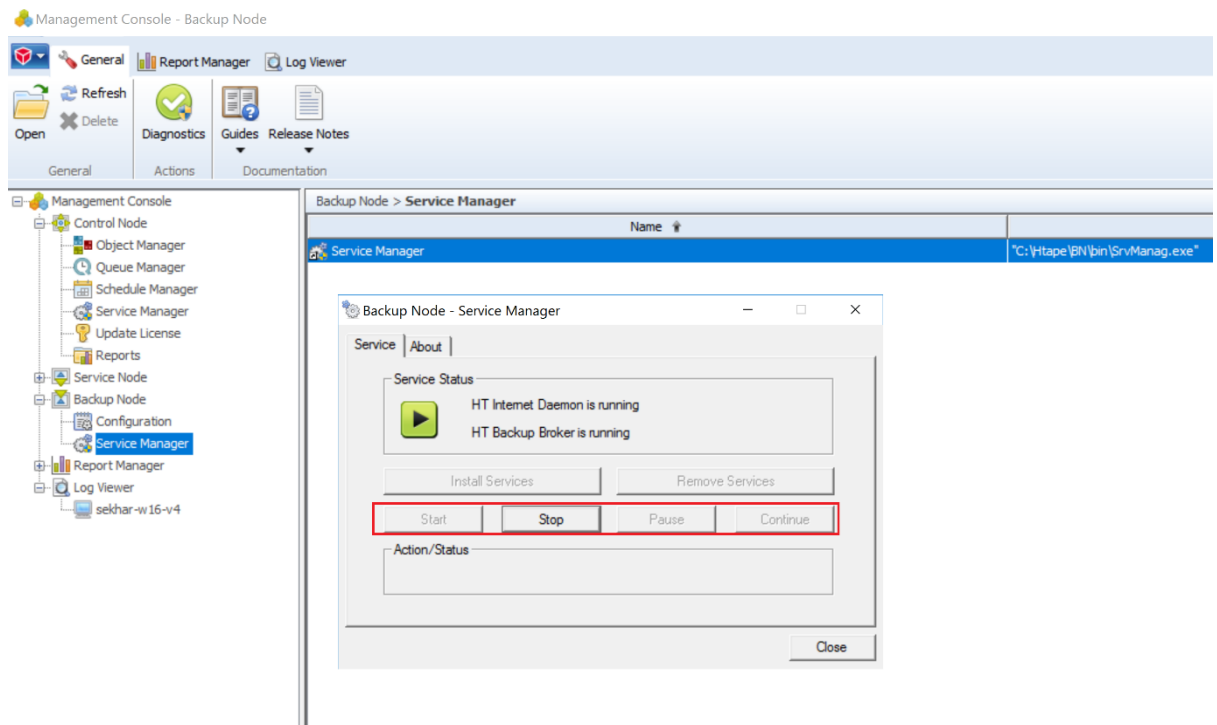
## 6. Restoring from the replication target

**i** **NOTE:** Before restoring from the target QoreStor system, make sure that the replication session state is INSYNC on the QoreStor system GUI Replication menu. Stop or Delete the replication session, and make sure that the target QoreStor system container has the CIFS/NFS connection(s) enabled.

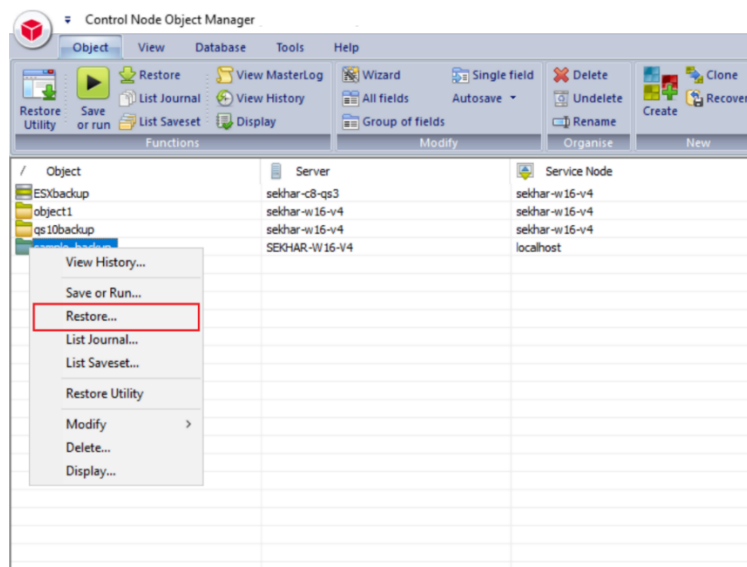
1. Add the target QoreStor system container to the BridgeHead :
2. 1. Click Configuration of Backup Node, which displays Configuration File, Double click to open the Configuration File. Modify the Stage Path to point to **the** target QoreStor container path, then save the changes.



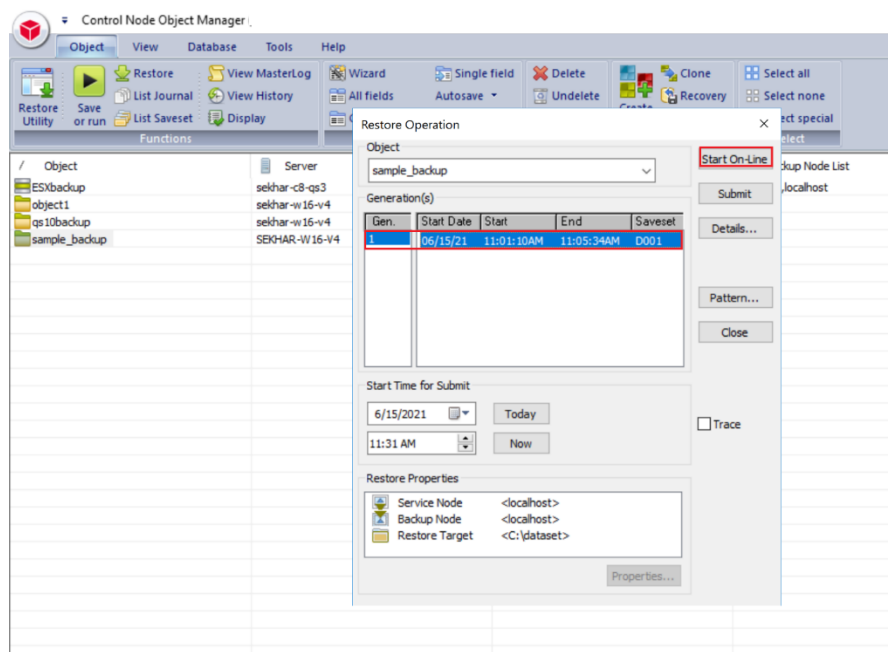
3. Go to Backup Node -> Service Manager, restart the Service of Backup Node.



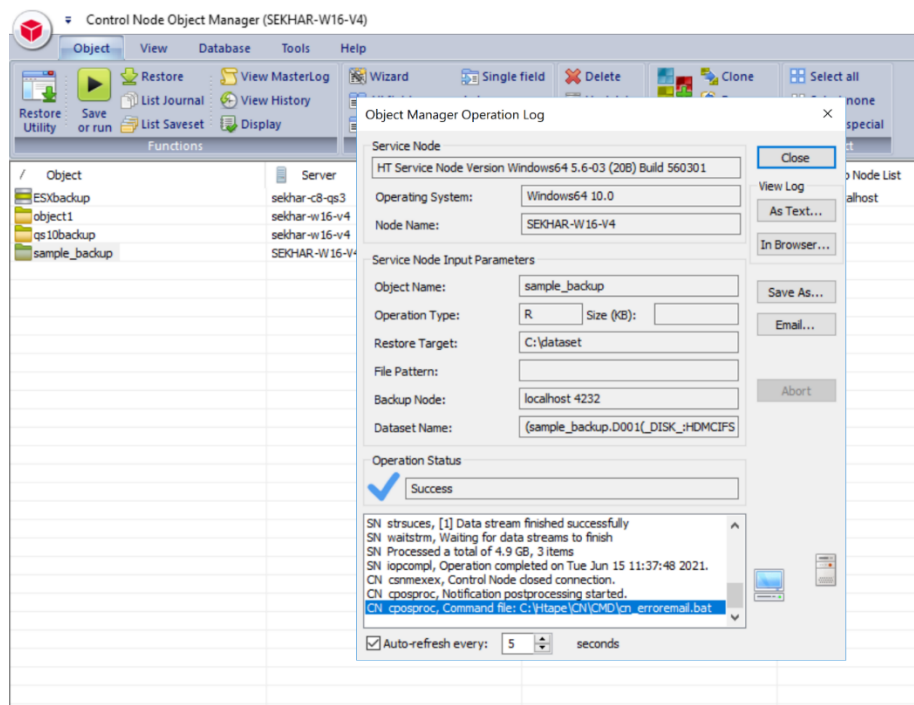
4. On BridgeHead Management Console, open Object Manager, and the backup object summary is displayed under the Object list. Right-click the object and SelectRestore



5. Select the Saveset, then click Start On-Line.

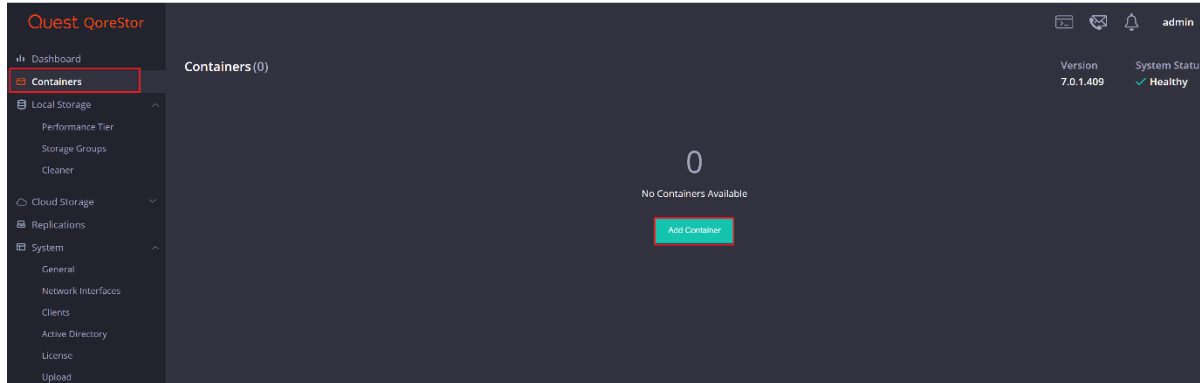


6. Verify that the restore job completes successfully.

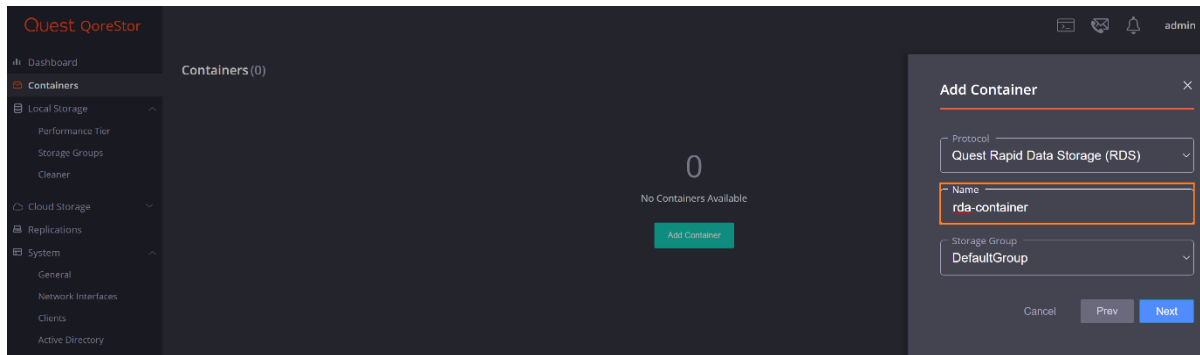


## 7. Creating RDS container for use with BridgeHead:

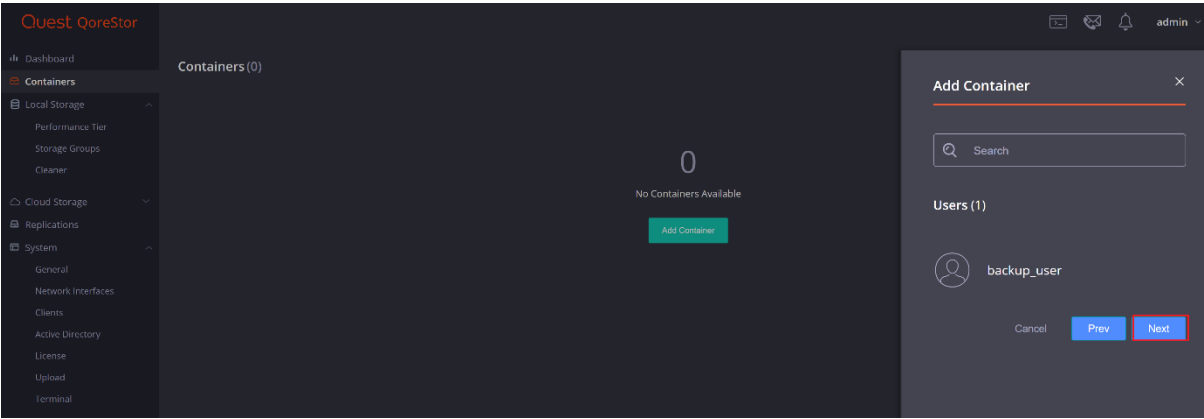
1. Select the Containers tab, then click Add container.



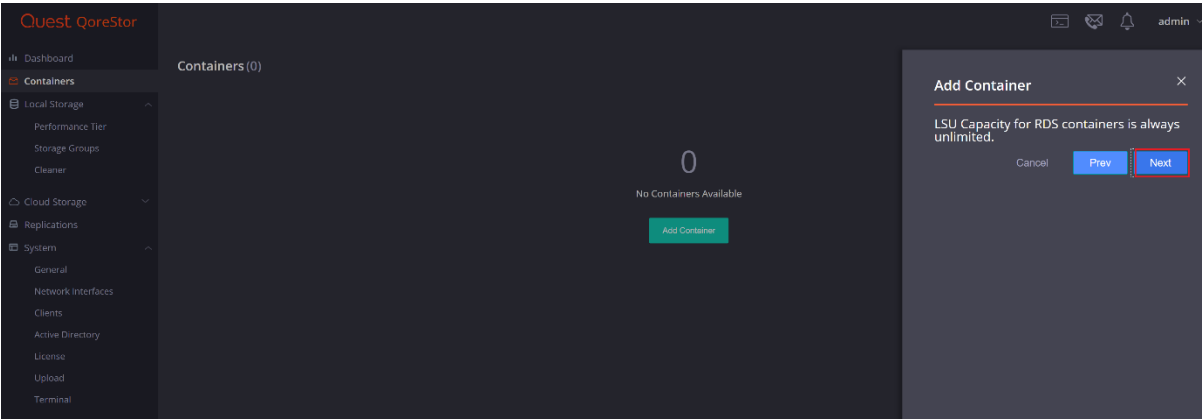
2 Enter a container Name, select a Storage Group or leave the DefaultGroup option selected, and select Quest Rapid Data Storage(RDS) from the Protocol dropdown menu. Click Next.



3. Accepts the Defaults and Click NEXT

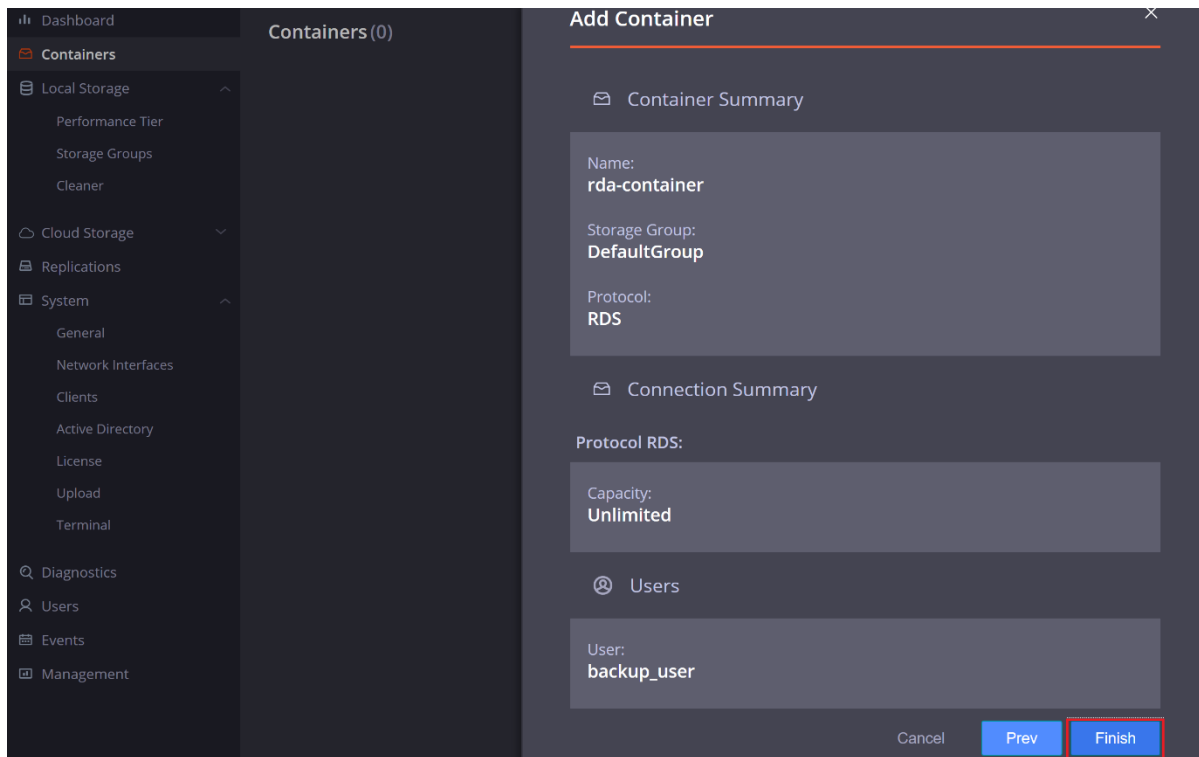


4. Accepts the Defaults and Click NEXT





5. Verify the container summary and click on Finish to add it



By default, QoreStor has a user with RDA Role named backup\_user and password "St0r@ge!". Refer to the *QoreStor User Guide* for information on changing user accounts.

## 8. Add RDS container to Bridgehead

1. Open the command prompt where BridgeHead is installed and go to the RDA folder.

```
c:\>cd c:\Htape\BN\cloud\rda
```

2. Run RDAUTIL.EXE

```
c:\Htape\BN\cloud\rda>rdutil.exe
```

3. Create an RDA instance to add the QoreStor RDS container.

```
c:\Htape\BN\cloud\rda>rdutil.exe
rdutil> add rda rdatarget1
RDA instance RDATARGET1 added OK

The instance has the following settings...

      Name: RDATARGET1
      Status: Uninitialized
      Server: (Blank, must be set)
      Port: 0
      Username: backup_user
      Password: *****
      Container: (Blank, must be set)
      Root directory: BridgeHead
      Write chunk size: 1024 KB
      Error limit: 5000
      Grace days: 5
      Secondary copy: (Blank)
      Tertiary copy: (Blank)
      Restore order: 123
      Daily job max concurrent jobs: 8
      Daily job progress check: 5 mins
      Daily job max replication time: 600 mins
      Daily job total run time: 900 mins
      Deduplication mode: Auto
      SecureConnect: On
      StorageGroup: DefaultGroup
```

#### 4. Set QoreStor Server name/IP.

```
rdutil> set rda rdatarget1 /server=10.230.48.240
Instance attributes changed OK, new details are...
Name: RDATARGET1
Status: Uninitialized
Server: 10.230.48.240
Port: 0
Username: backup_user
Password: *****
Container: (Blank, must be set)
Root directory: BridgeHead
Write chunk size: 1024 KB
Error limit: 5000
Grace days: 5
Secondary copy: (Blank)
Tertiary copy: (Blank)
Restore order: 123
Daily job max concurrent jobs: 8
Daily job progress check: 5 mins
Daily job max replication time: 600 mins
Daily job total run time: 900 mins
Deduplication mode: Auto
SecureConnect: On
StorageGroup: DefaultGroup
Logging: No
Flags: 00000000 (=0 decimal)
Comment: (Blank)
rdutil> 
```

## 5. Set QoreStor Storage Group.

```
rdautl> set rda rdatarget1 /storage=DefaultGroup

Instance attributes changed OK, new details are...

      Name: RDATARGET1
      Status: Uninitialized
      Server: 10.230.48.240
      Port: 0
      Username: backup_user
      Password: *****
      Container: (Blank, must be set)
      Root directory: BridgeHead
      Write chunk size: 1024 KB
      Error limit: 5000
      Grace days: 5
      Secondary copy: (Blank)
      Tertiary copy: (Blank)
      Restore order: 123
      Daily job max concurrent jobs: 8
      Daily job progress check: 5 mins
      Daily job max replication time: 600 mins
      Daily job total run time: 900 mins
      Deduplication mode: Auto
      SecureConnect: On
      StorageGroup: DefaultGroup
      Logging: No
      Flags: 00000000 (=0 decimal)
      Comment: (Blank)

rdautl>
```

## 6. Set QoreStor RDS Container.

```
rdutil> set rda rdatarget1 /container=rda-container
Instance attributes changed OK, new details are...

      Name: RDATARGET1
      Status: Uninitialized
      Server: 10.230.48.240
      Port: 0
      Username: backup_user
      Password: *****
      Container: rda-container
      Root directory: BridgeHead
      Write chunk size: 1024 KB
      Error limit: 5000
      Grace days: 5
      Secondary copy: (Blank)
      Tertiary copy: (Blank)
      Restore order: 123
      Daily job max concurrent jobs: 8
      Daily job progress check: 5 mins
      Daily job max replication time: 600 mins
      Daily job total run time: 900 mins
      Deduplication mode: Auto
      SecureConnect: On
      StorageGroup: DefaultGroup
      Logging: No
      Flags: 00000000 (=0 decimal)
      Comment: (Blank)

rdutil> _
```

7. Initialize the RDA instance.

```
rdutil> init rda rdatarget1
Backup Node software located at C:\Htape\BN
Attempting to connect to server...
Connected OK!
Created /BridgeHead/BH1/RDATARGET1/CNTRL
Created /BridgeHead/BH1/RDATARGET1/CNTRL/Replication/Copy2/CopyPending
Created /BridgeHead/BH1/RDATARGET1/CNTRL/Replication/Copy3/CopyPending
Created /BridgeHead/BH1/RDATARGET1/CNTRL/Replication/Copy2/DeletePending
Created /BridgeHead/BH1/RDATARGET1/CNTRL/Replication/Copy3/DeletePending
Created /BridgeHead/BH1/RDATARGET1/DATA
RDATARGET1 initialized and ready for use

To set a Control Node object to use this instance set its media
details to the values below...

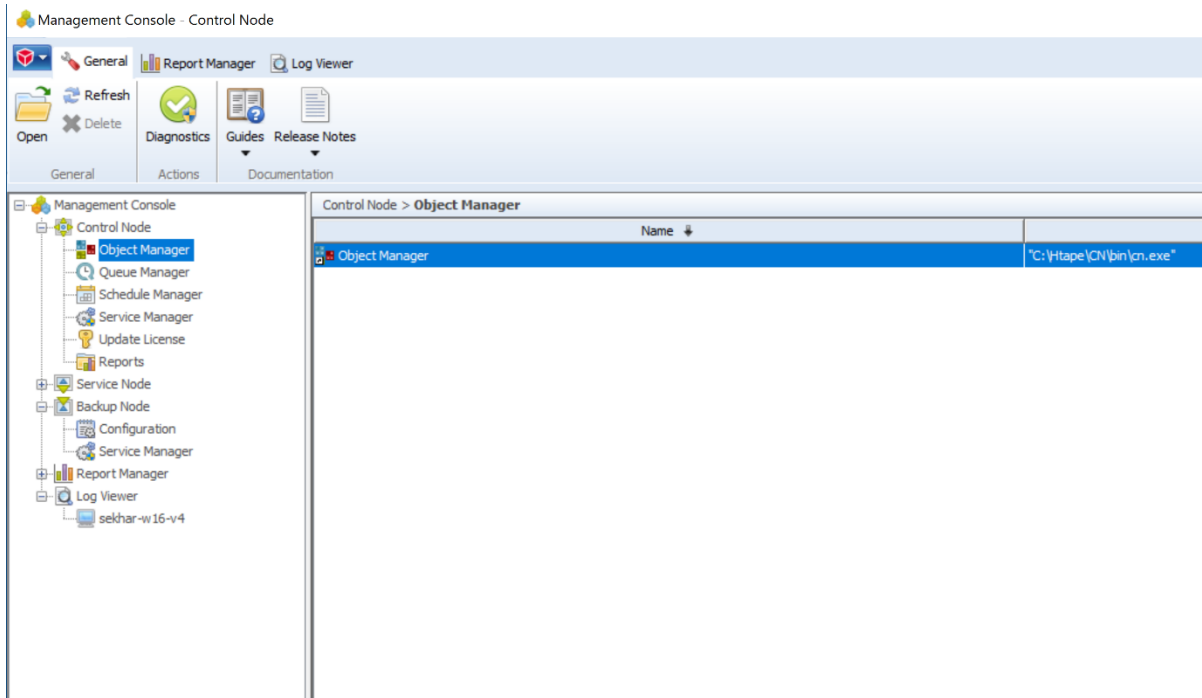
Option:   Cloud
Type:     RDA
Instance: RDATARGET1

rdutil>
```

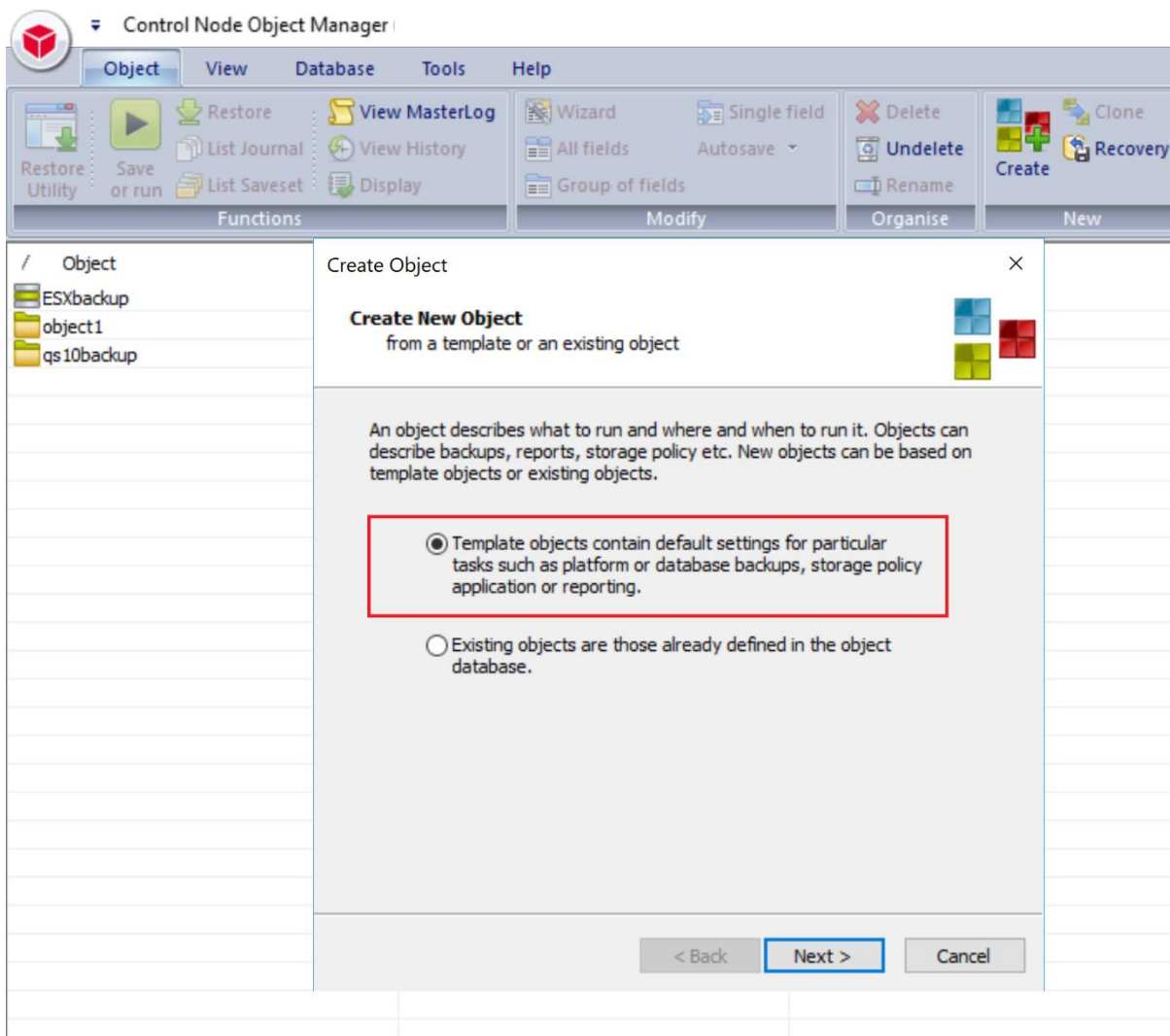
8. Exit.

```
rdutil> exit
```

9. On Bridge Head Management Console, click Object Manager under Control Node, which displays the Object Manager in the list. Double-click to open the Object Manager on right- hand side pane.

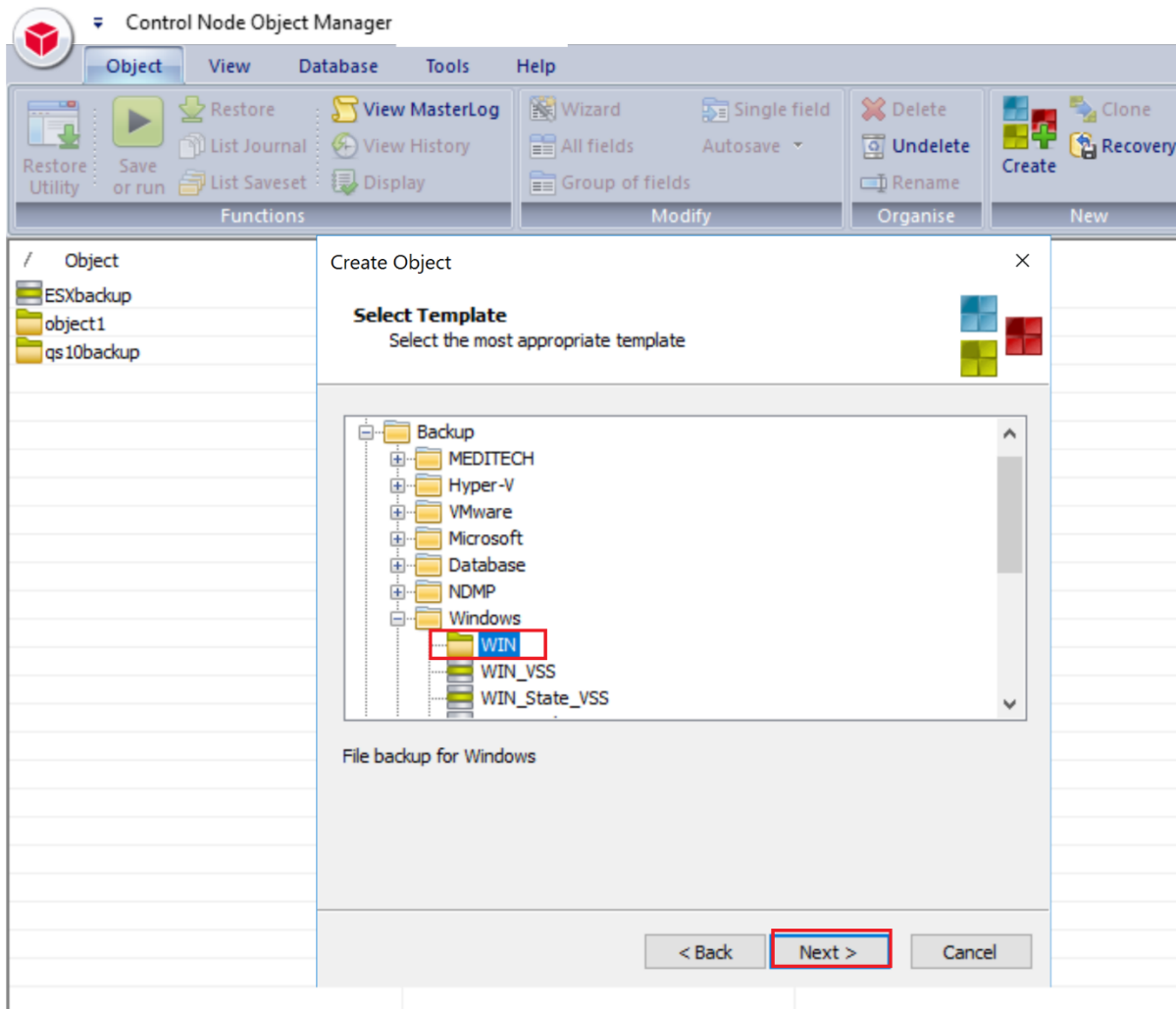


10. Select Template objects to contain default settings for particular tasks such as platform or database backups, storage policy applications, or reporting, and click Next.





11. Select WIN in the template list then click Next.



12. Enter the Service Node related info with the valid file path for the backup data source, click on Credential manager to set the password and then click Next

**Control Node Object Manager**

Object View Database Tools Help

Restore Utility Save or run List Journal List Saveset Display View MasterLog View History Display Wizard All fields Group of fields Single field Autosave Delete Undelete Rename Create Clone Recovery

**Create Object**

**Service Node**

A Service Node is a computer whose data is saved or restored by an operation initiated a Control Node. During a save, data is collected and sent to a Backup Node.

Computer: localhost

Credential: administrator

Credential Manager...

Path defines data to be saved or restored

Path: C:\dataset

< Back Next > Cancel

### 13. Enter Backup Node related info

The screenshot shows the 'Control Node Object Manager' application. The 'Create Object' dialog box is open, displaying the 'Backup Node List' section. The dialog has a title bar with a close button (X). Below the title bar, there's a section titled 'Backup Node List' with a warning icon. The text below the title reads: 'Backup Nodes store data on disk or tape. If you specify more than one node, Save operations that fail are automatically rerun on the next node. Repeat the same node for simple automatic retry.'

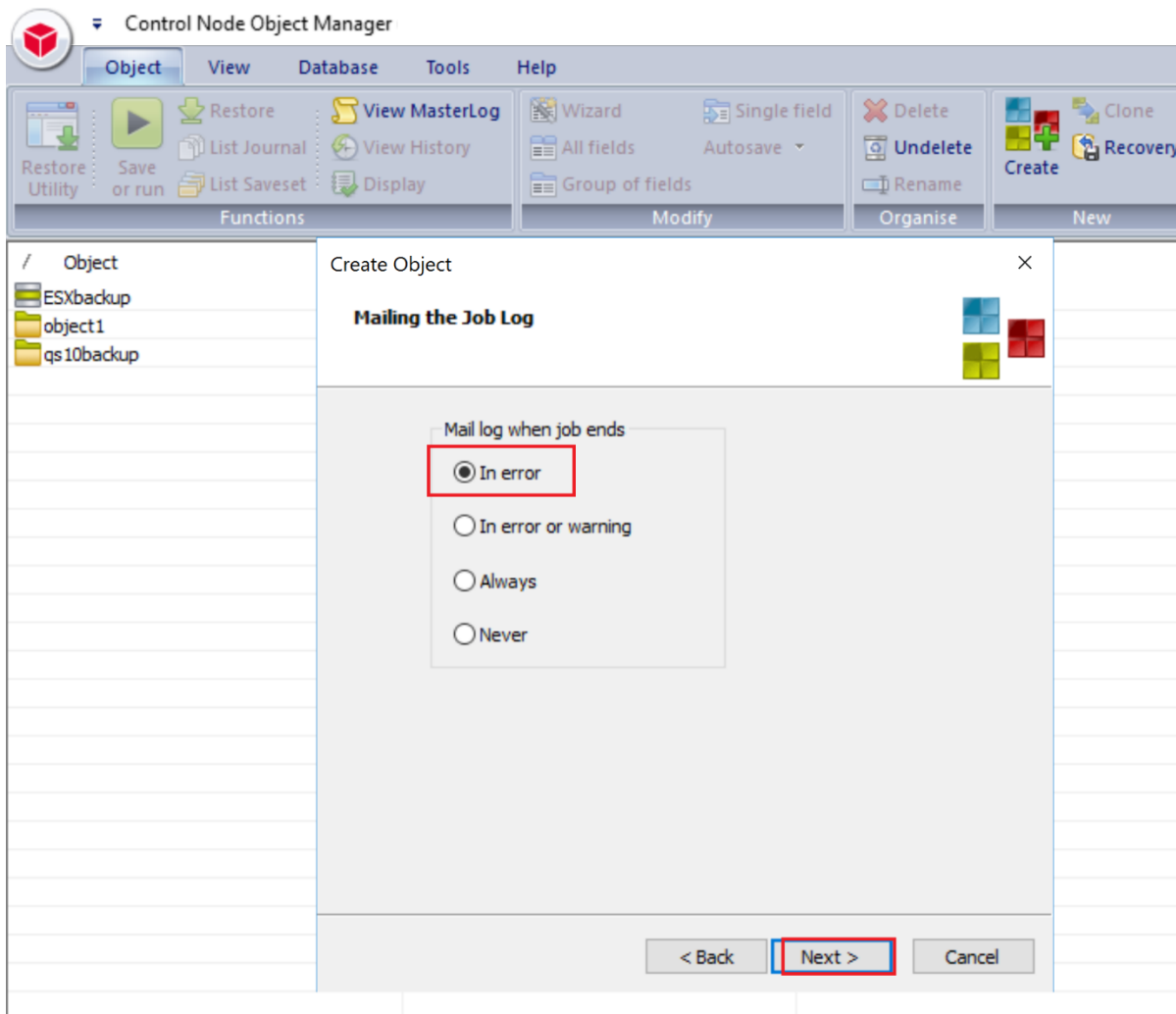
There are two columns for entering backup node information:

- 1st Computer and Credential:** This column has two dropdown menus. The first dropdown is highlighted with a red box and contains the text 'localhost'. The second dropdown contains the text 'administrator'.
- 2nd Computer and Credential:** This column has two empty dropdown menus.

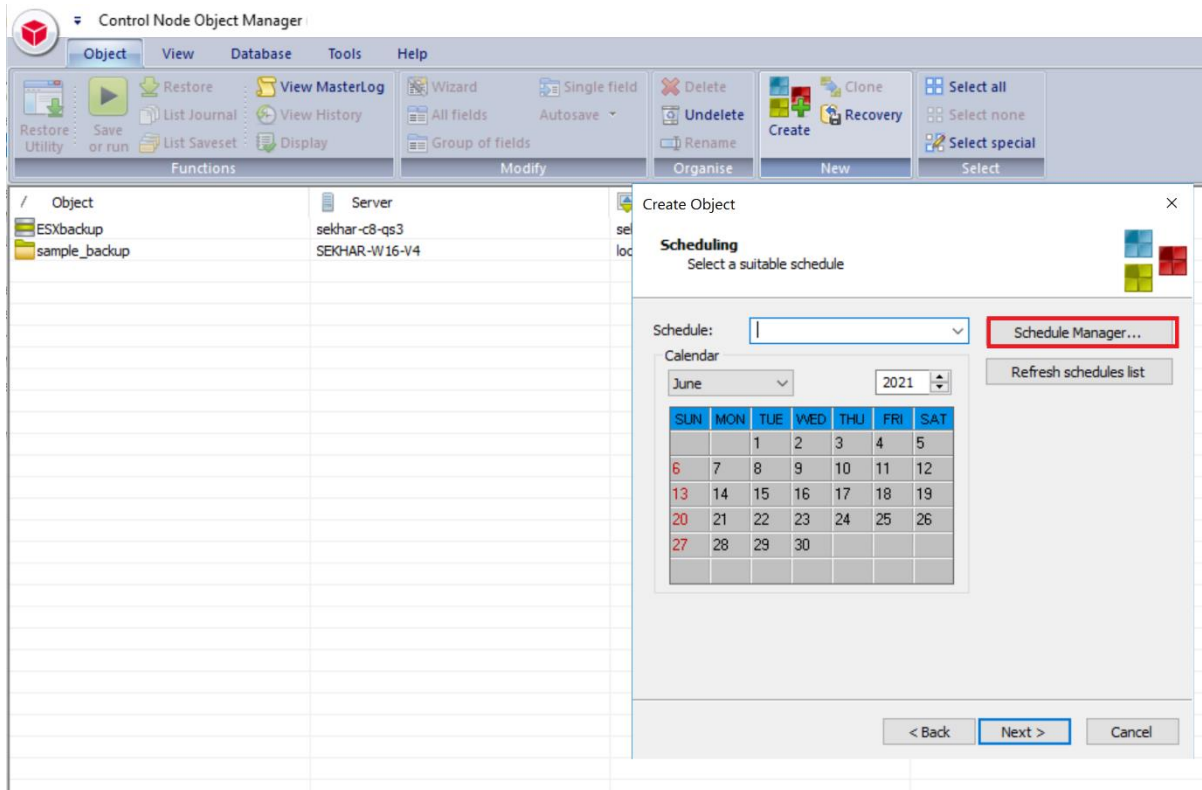
Below the dropdown menus, there are two buttons: 'Additional Backup Nodes...' and 'Credential Manager...'.

At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

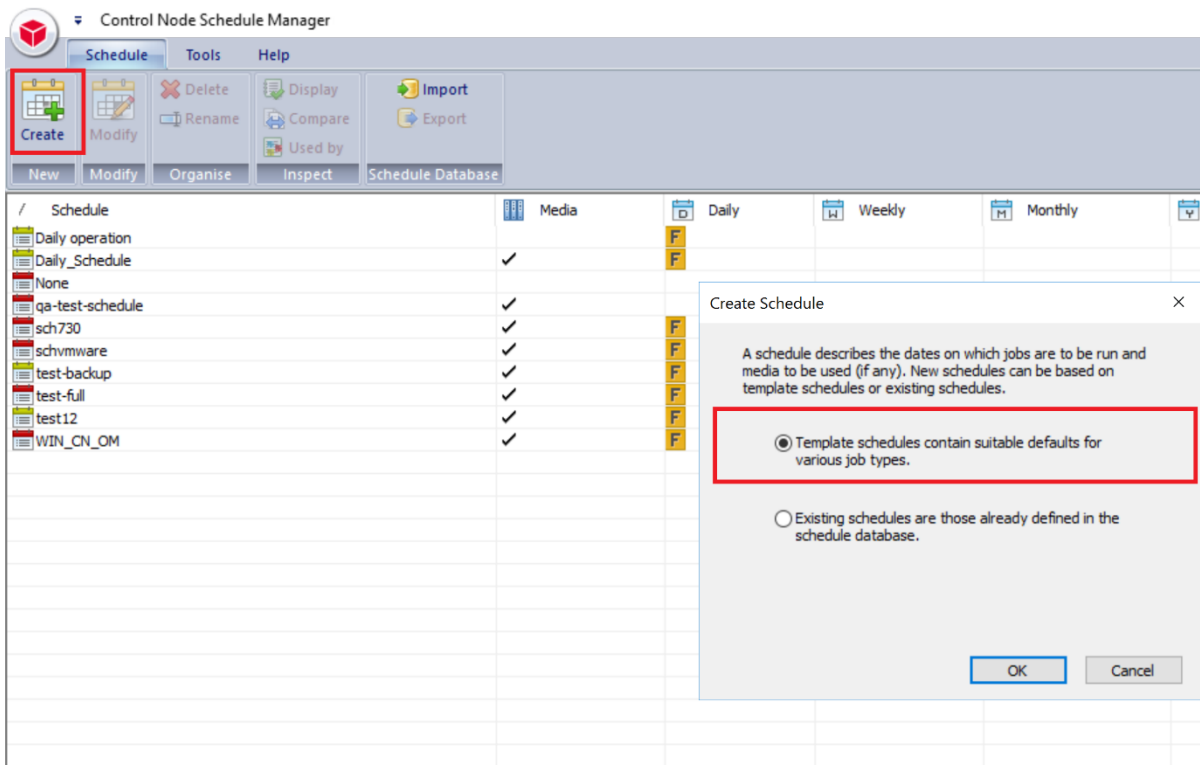
14. Accept the defaults and click NEXT.



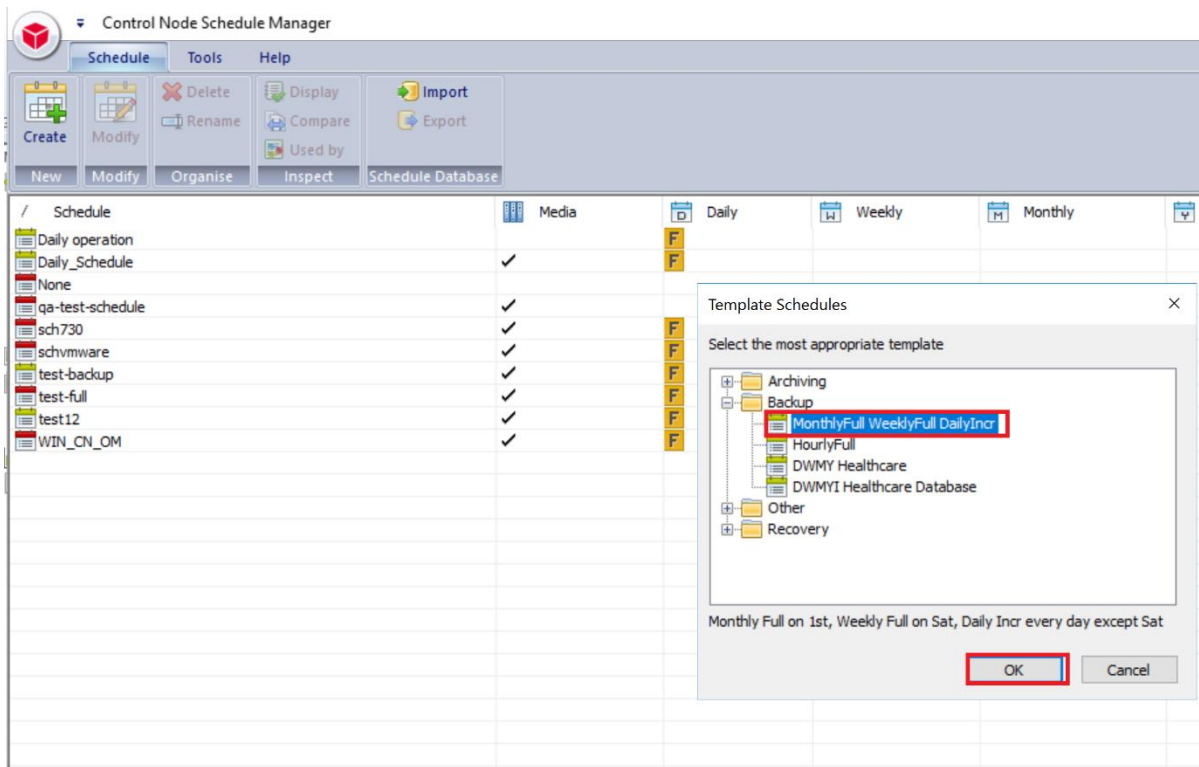
15. Click on schedule manager to create a schedule for the RDS backup.



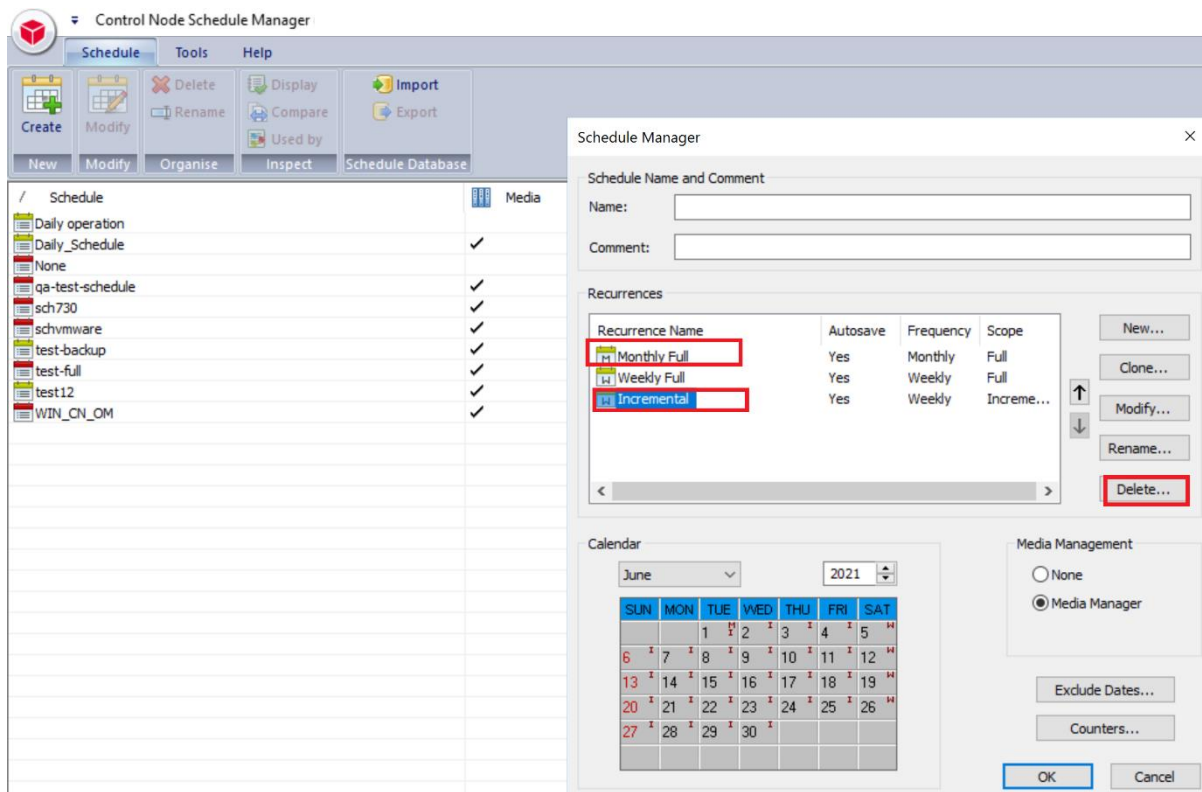
16. It will open schedule manager windows and SelectTemplate schedules to contain suitable defaults for various job types.  
Click OK.



17. Select template schedule MonthlyFullWeeklyFullDailyIncr and click **OK**.

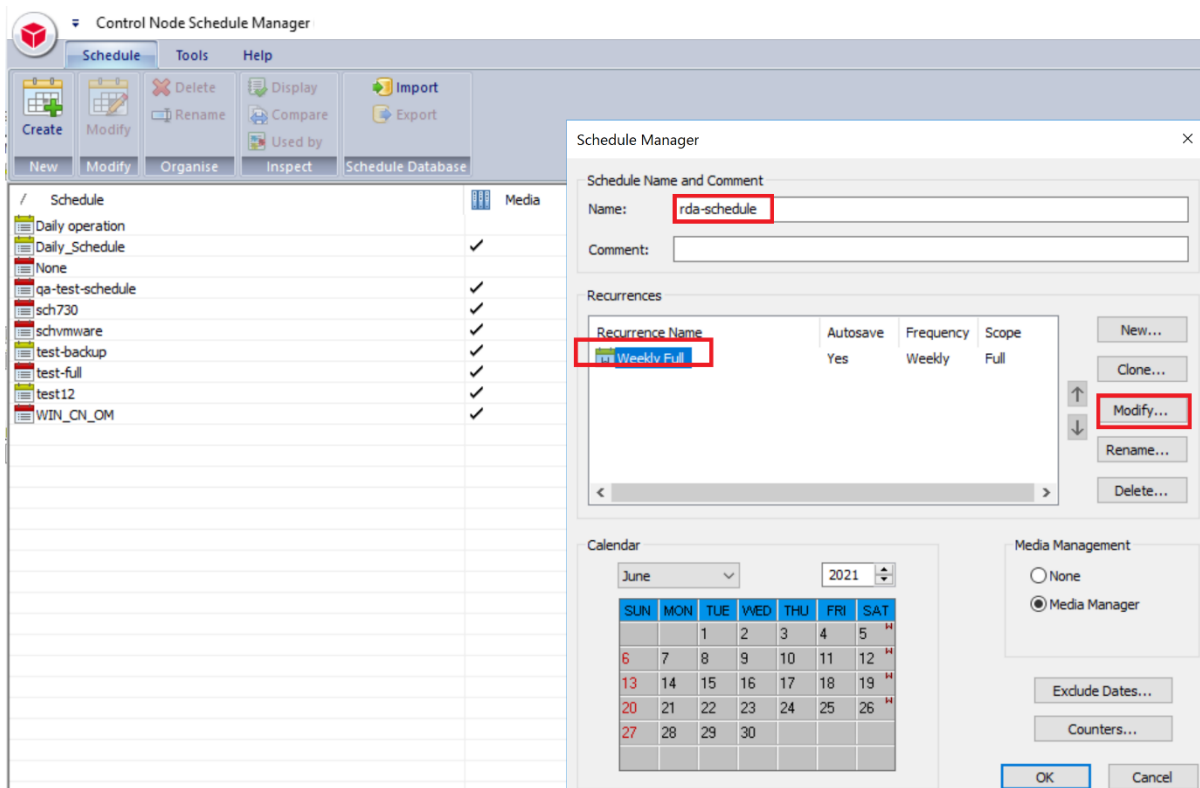


18. Delete monthly, Incremental schedules and keep Weekly full to modify it.

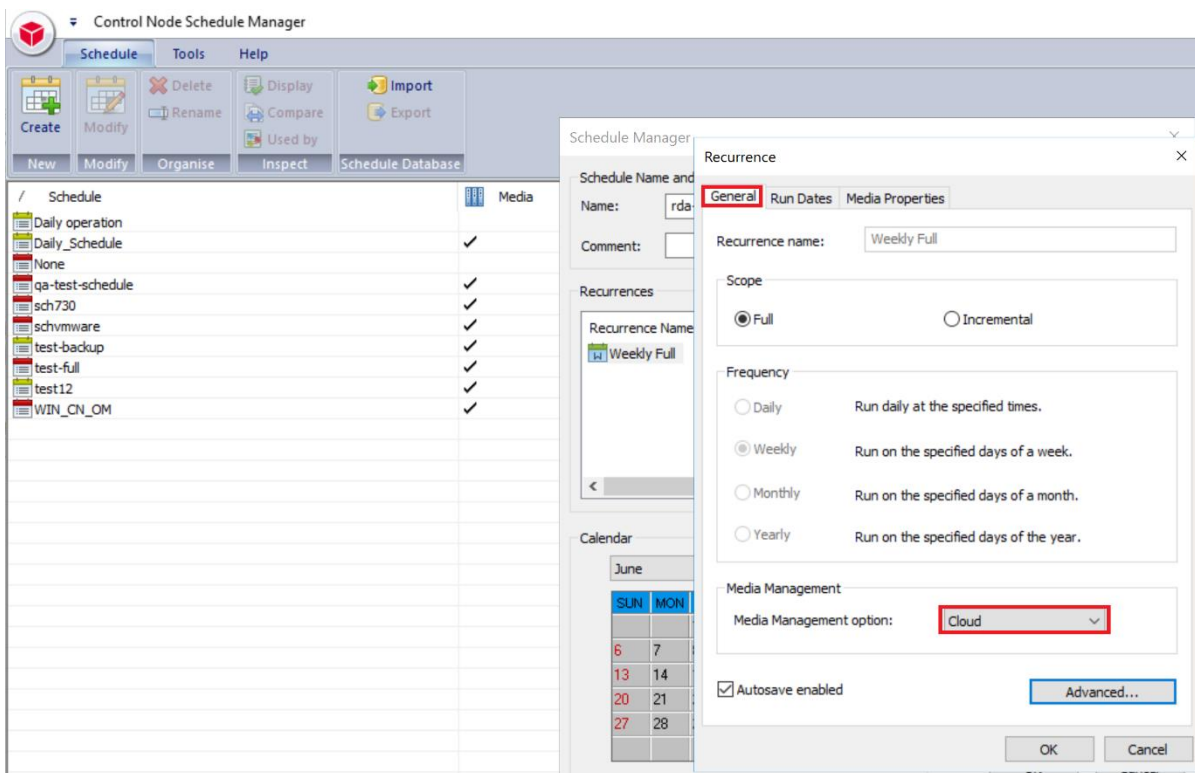




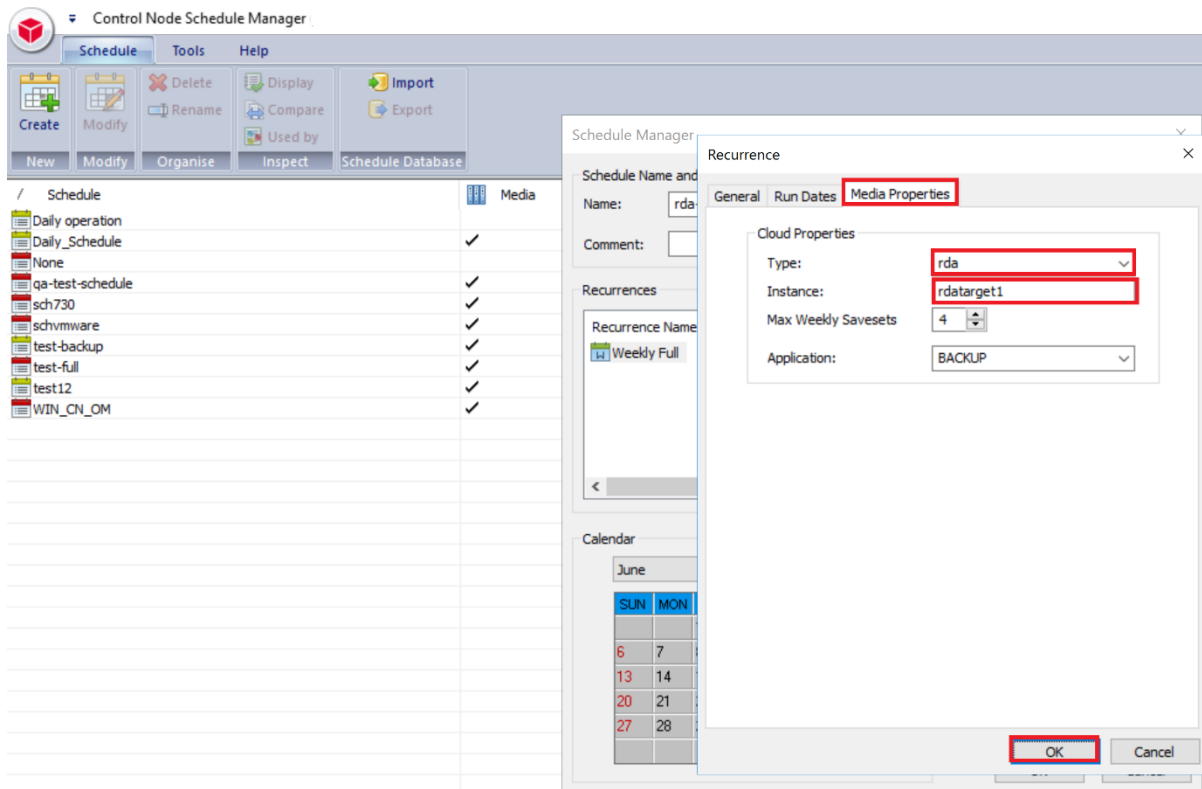
19. Enter the schedule name, select the weekly schedule, and then click on modify.



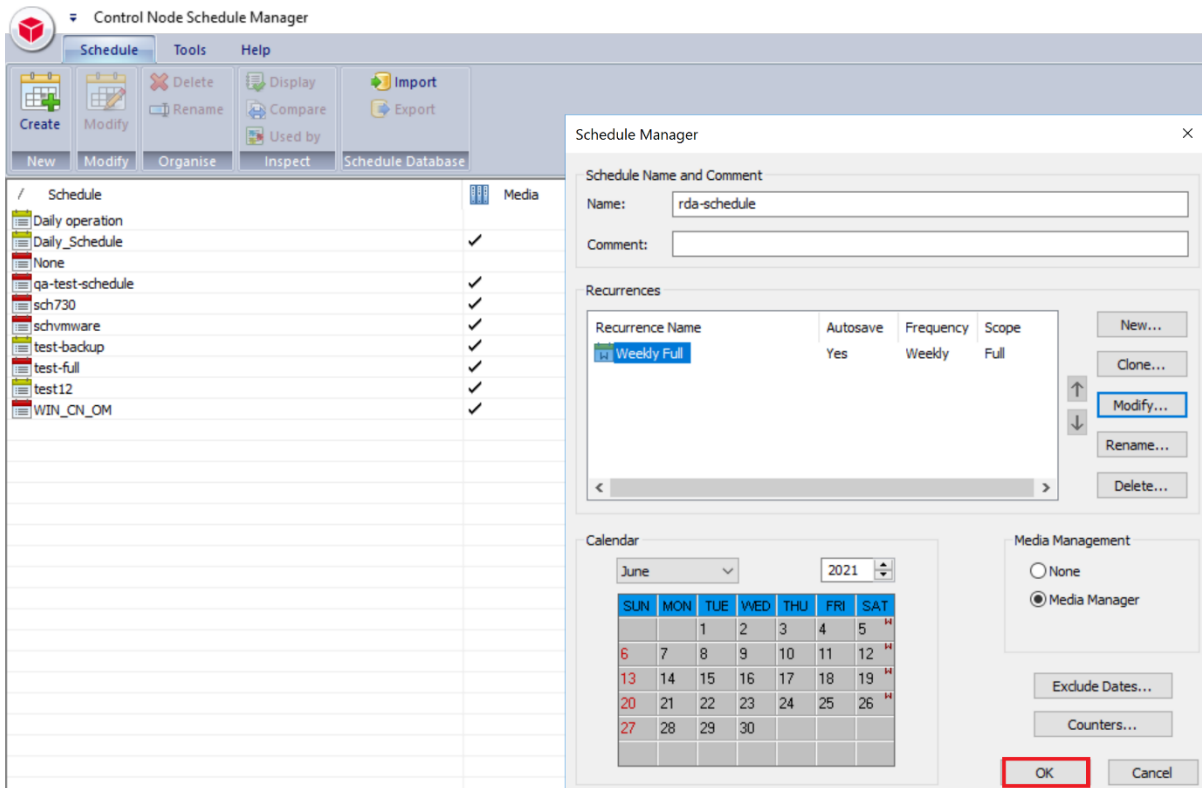
20. Select the **cloud** in the media management option under the general page.



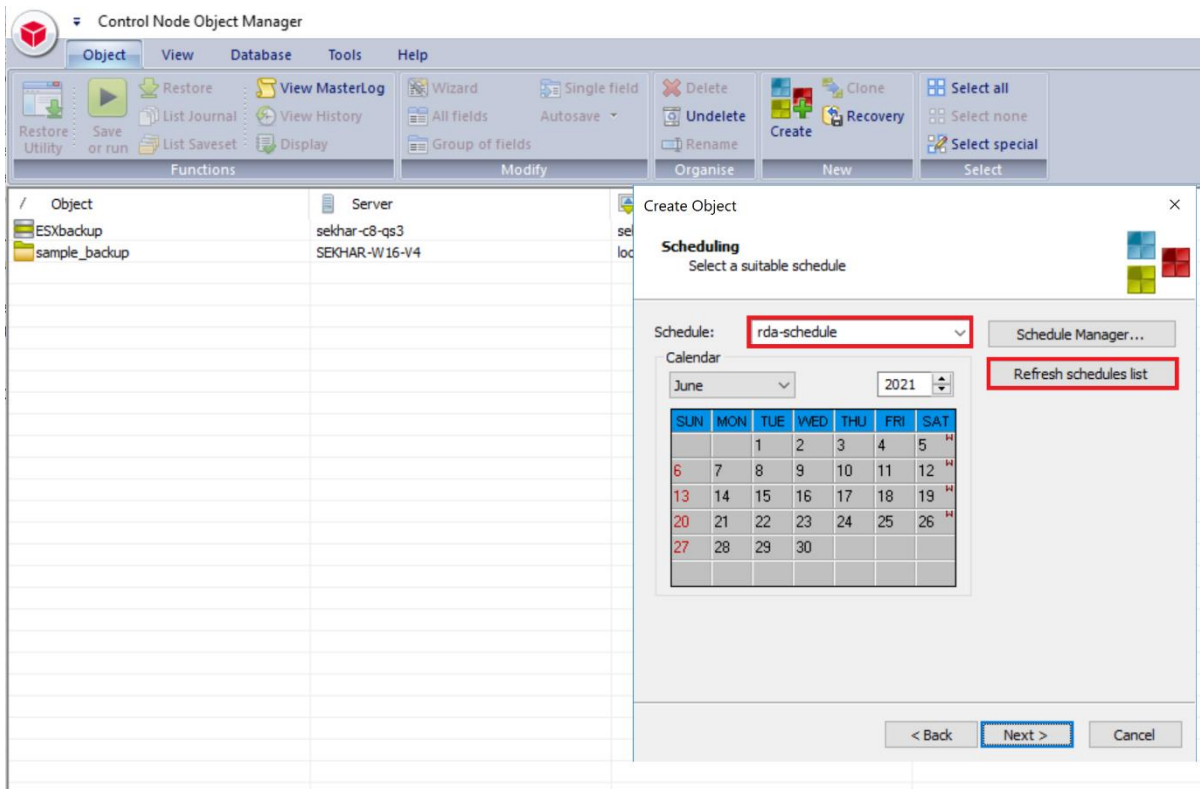
21. Select **RDA** as type, Enter **Instance** as the Name of the instance created using **RDAUTIL.exe** under Media Properties Page then click OK



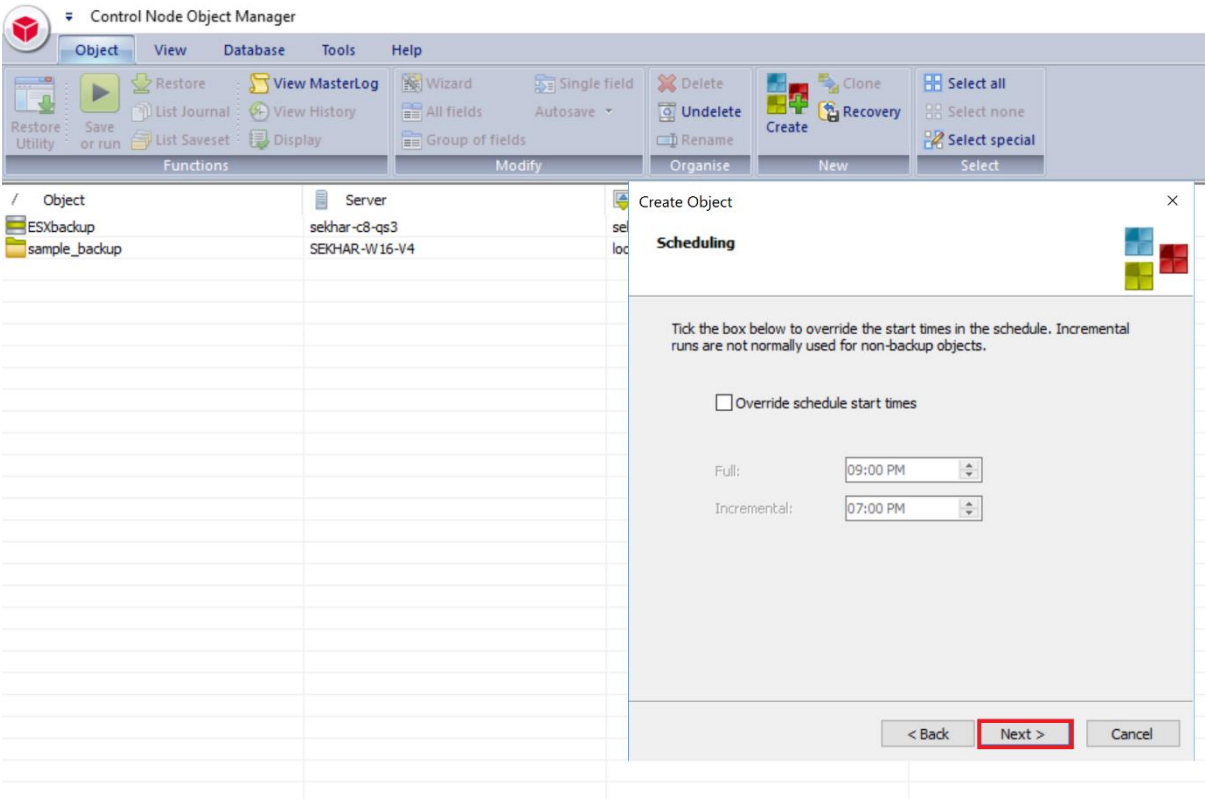
22. Click **OK** to save it.



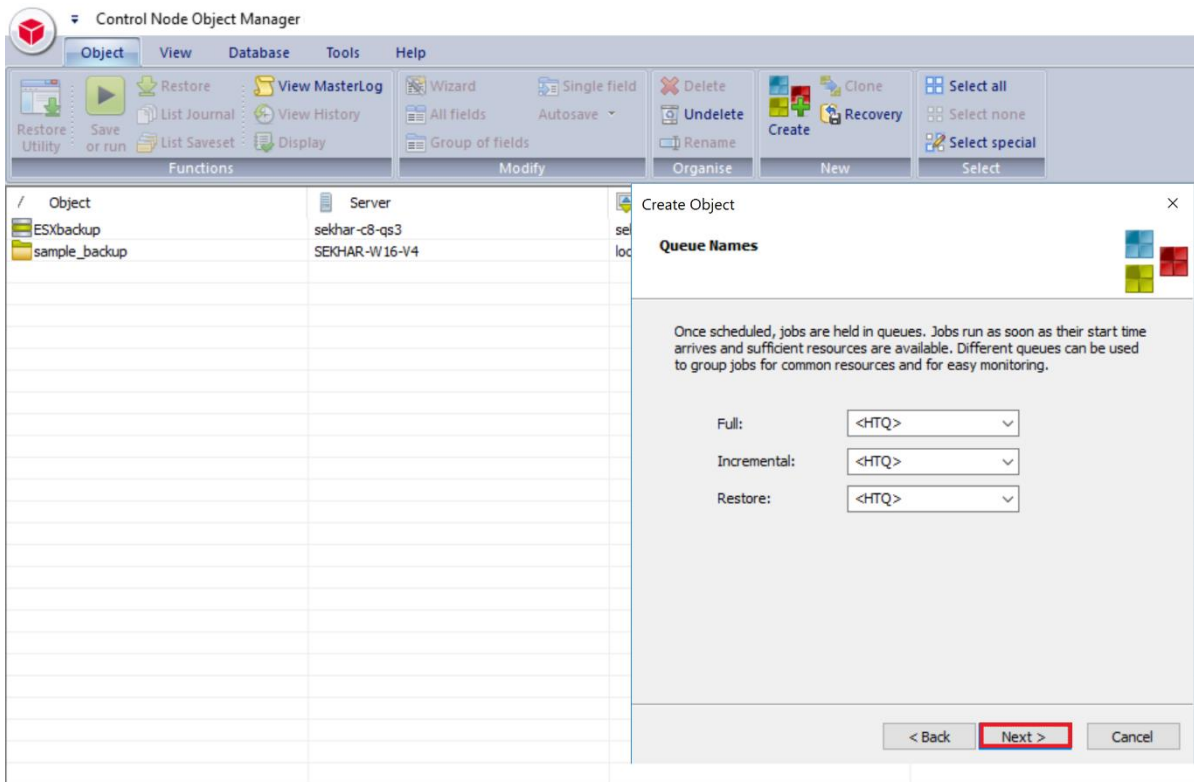
23. Click on the refresh schedule list to select the newly created schedule.



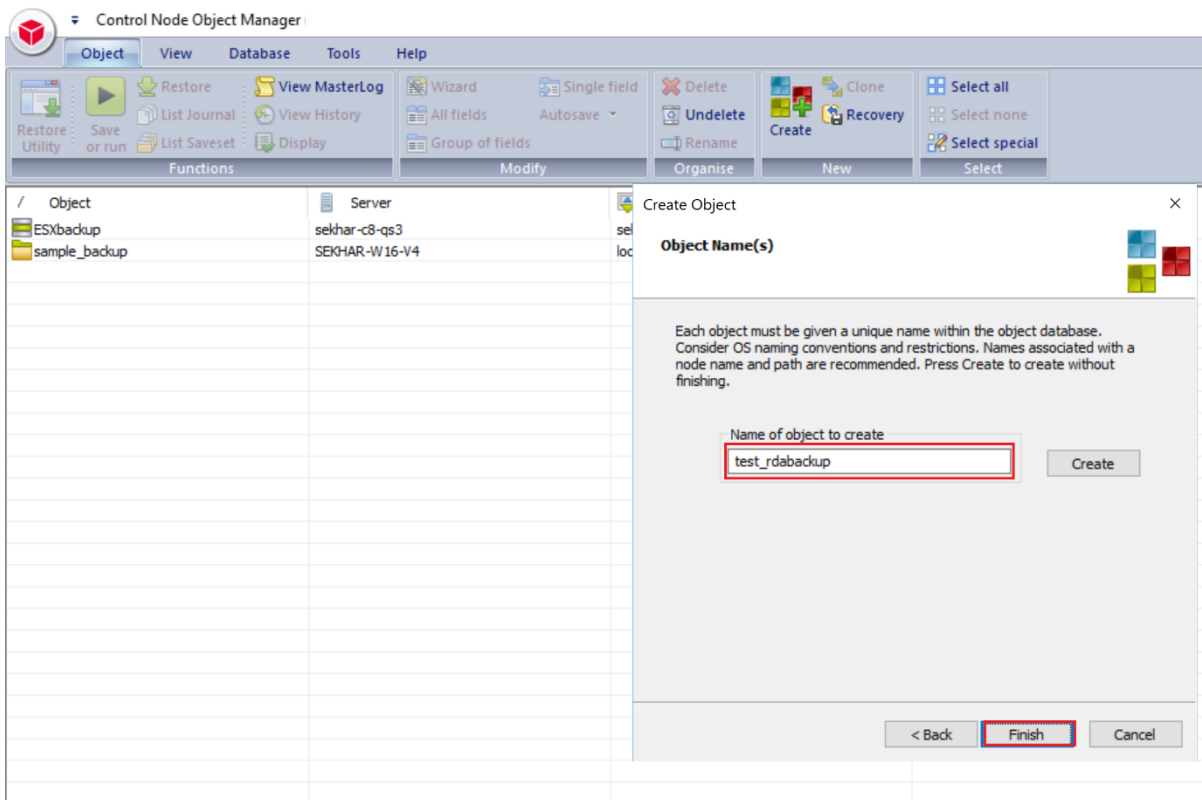
24. Accept default settings, click Next.



25. Accept defaults, click Next.

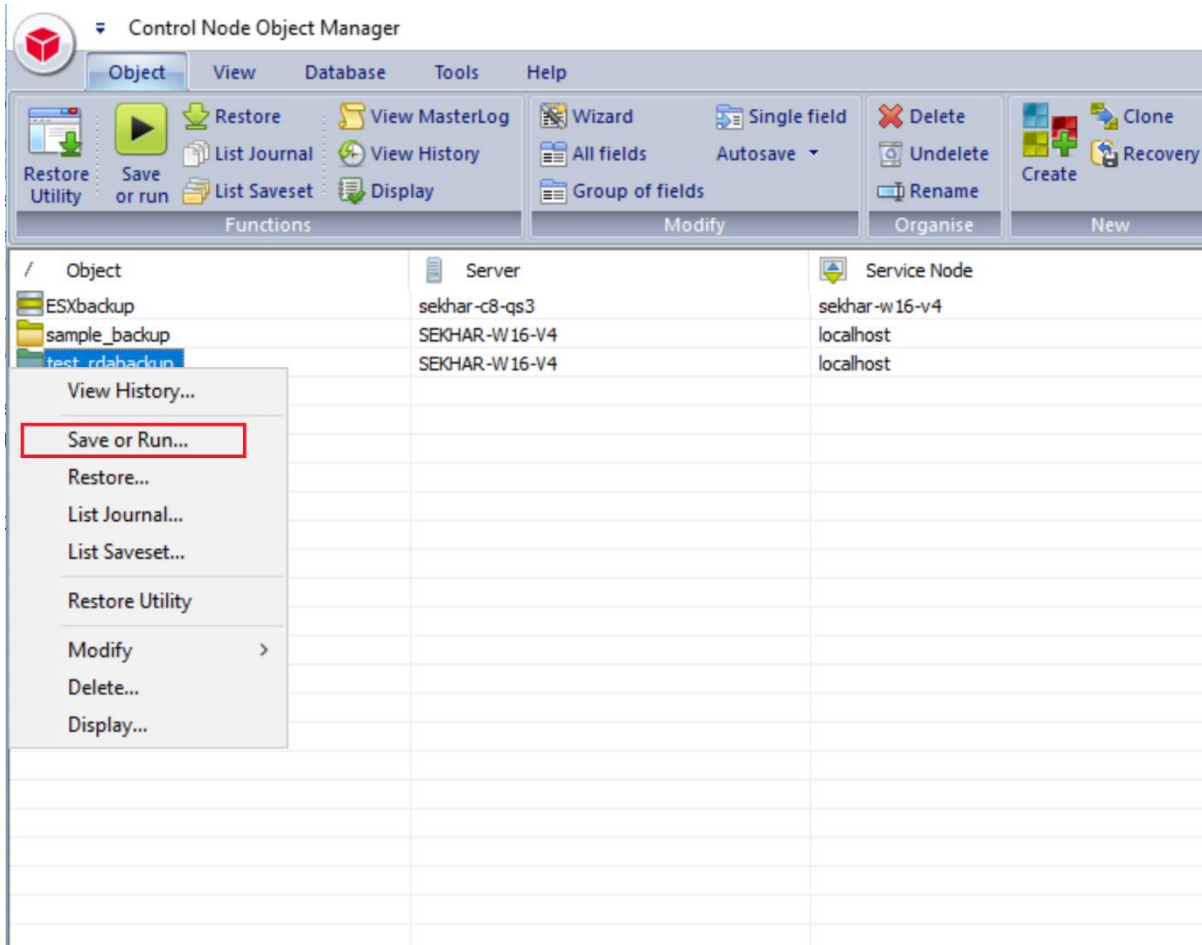


26. Enter the object name then click Finish.

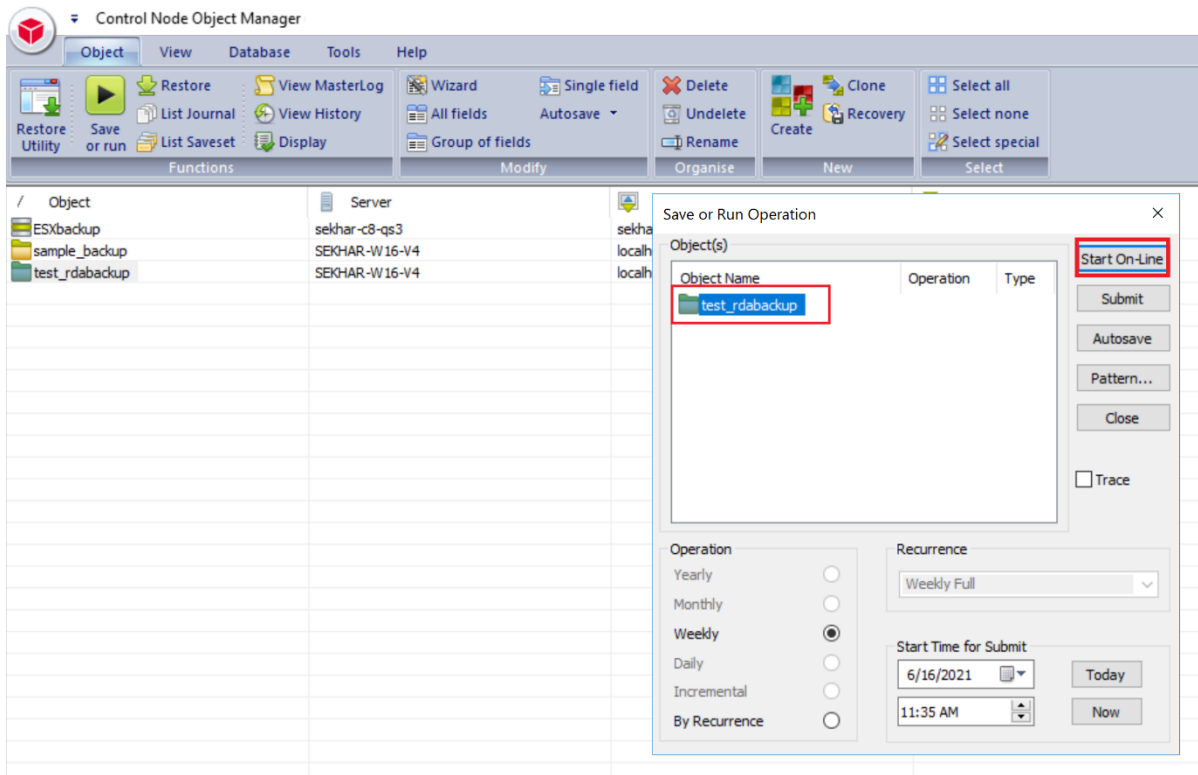




27. The backup object summary is displayed on the Object list. Right-click the object to run the backup.

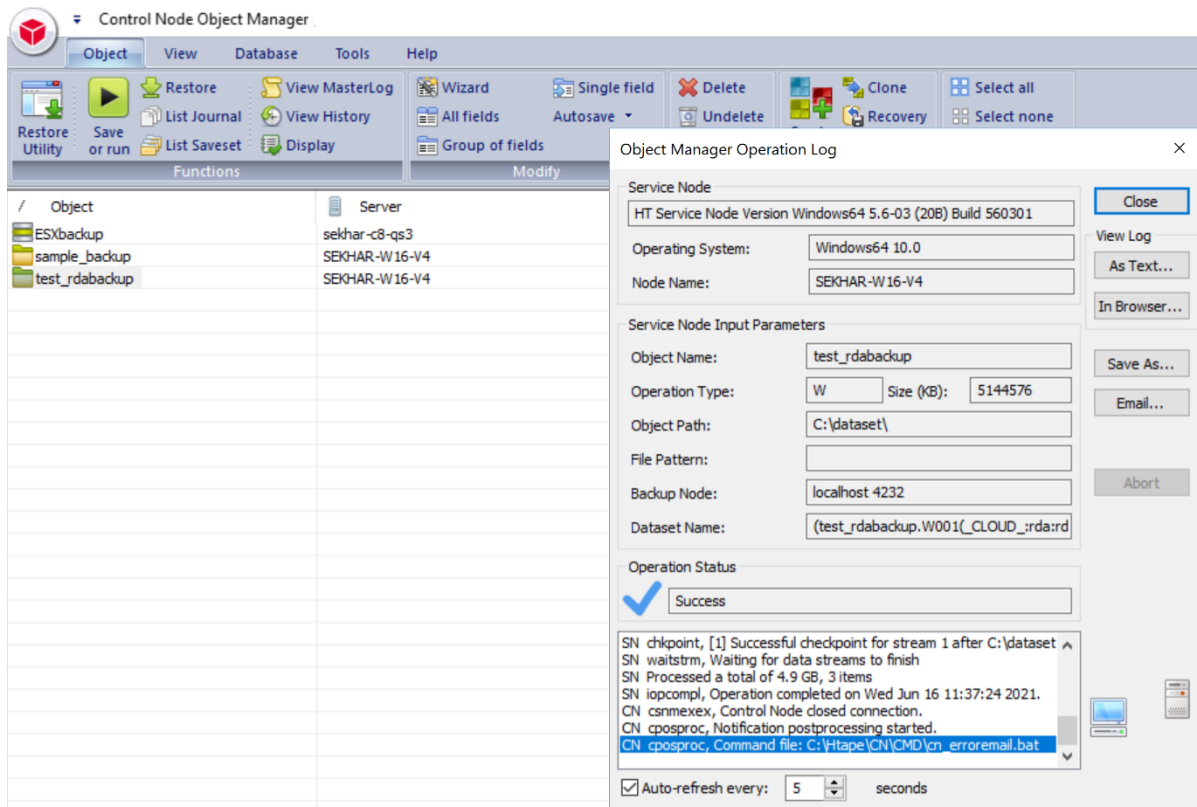


28. When Save or Run Operation window opens, click Start On-Line to start the backup.



29. The Object Manager Operation Log window displays the progress of the backup session.

Operation status has details of the backup job.

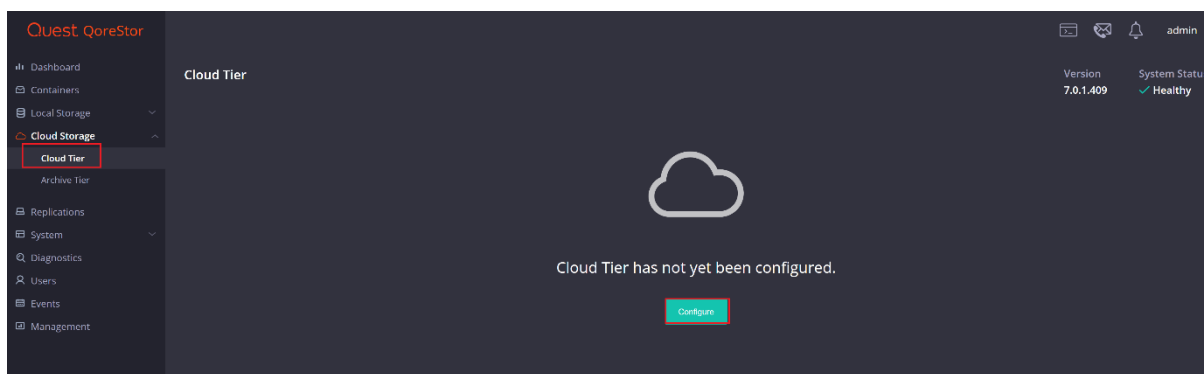


## 9. Setting up Cloud Tier

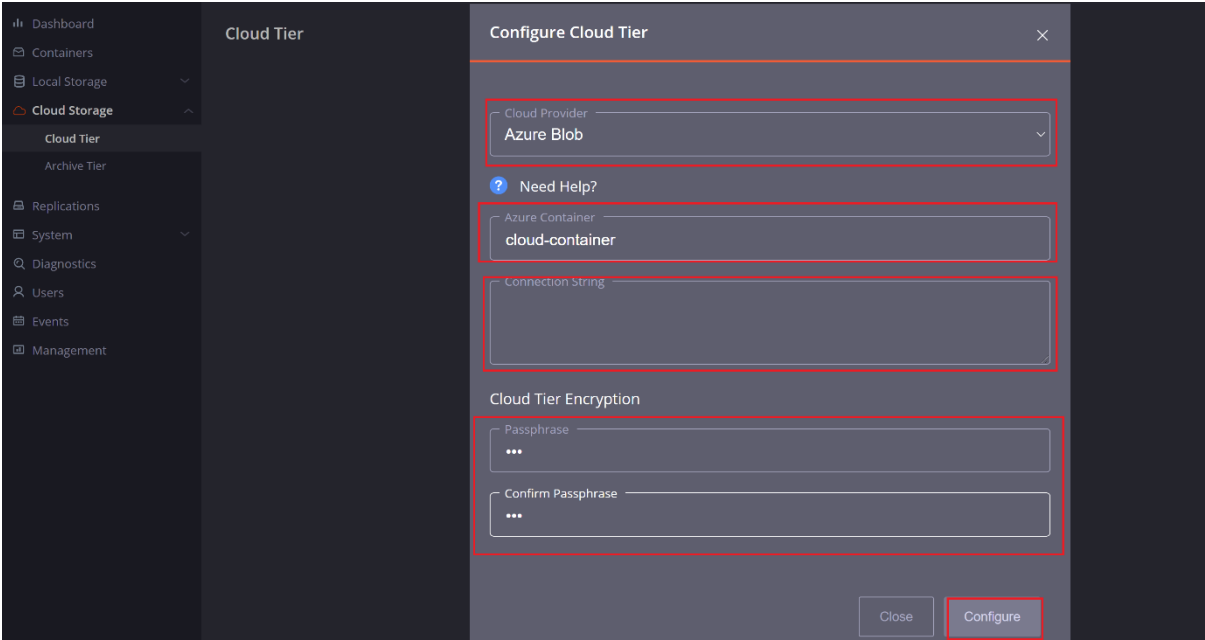
### Creating a policy-driven Cloud Tier

Cloud Tier is a feature that allows a QoreStor system to tier deduplicated blocks of files to a cloud provider via S3 protocol. There are several cloud and on-prem solution providers supported including Azure, AWS, Wasabi, IBM, Google, and many other S3-compatible solutions. Once added one or more containers can be added to a policy. How that policy is configured can determine how long the data is available on-prem in QoreStor, how long it's available both on-prem and in the cloud simultaneously, and finally at what point is it only available in the cloud.

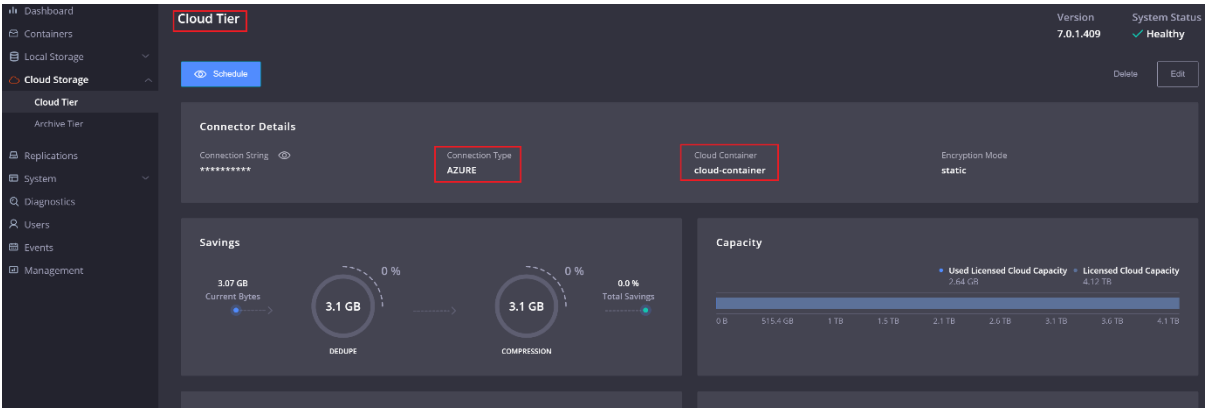
1. Open the QoreStor UI, expand the **Cloud Storage** section, and select the **Cloud Tier** page. Click the **Configure** button.



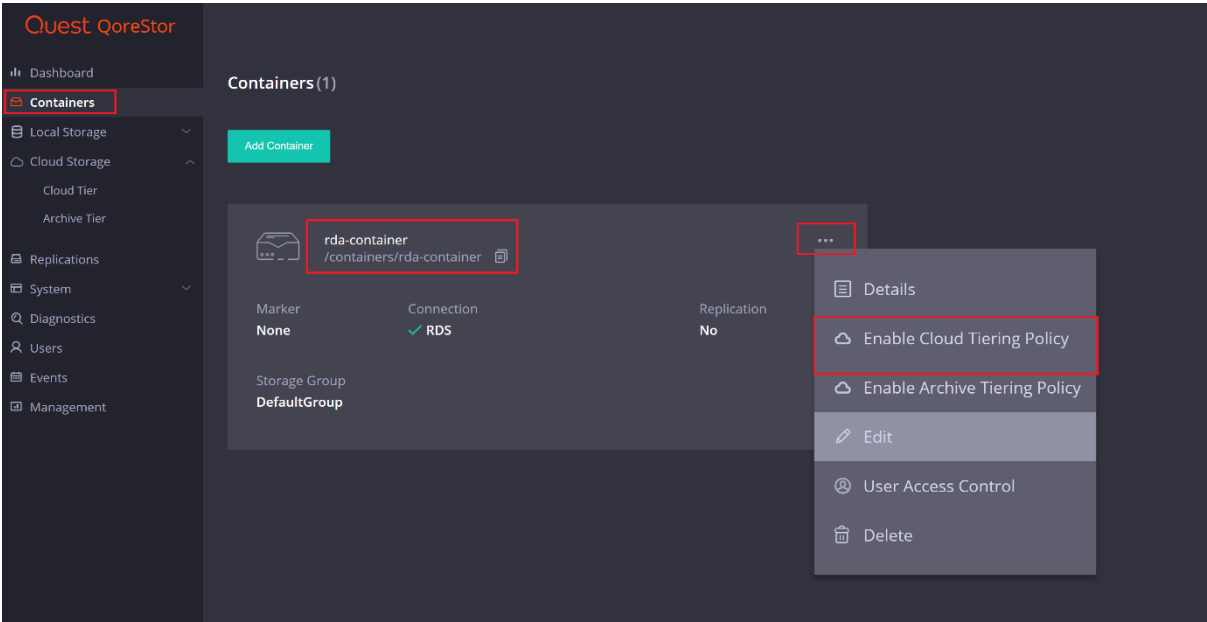
2. For Azure enter your Azure Container name, this will be created automatically in the cloud. Enter your Connection string from the Azure portal and your passphrase. This passphrase is user-defined and used to securely encrypt all files written to the cloud provider. Finally, click Configure.



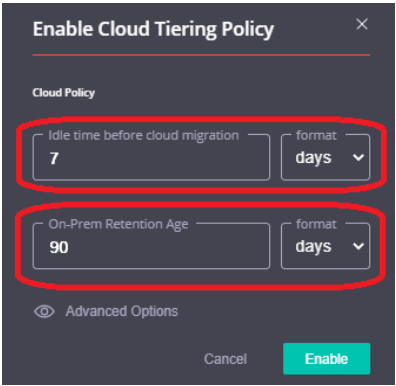
3. Once added this is how the cloud tier page should display.



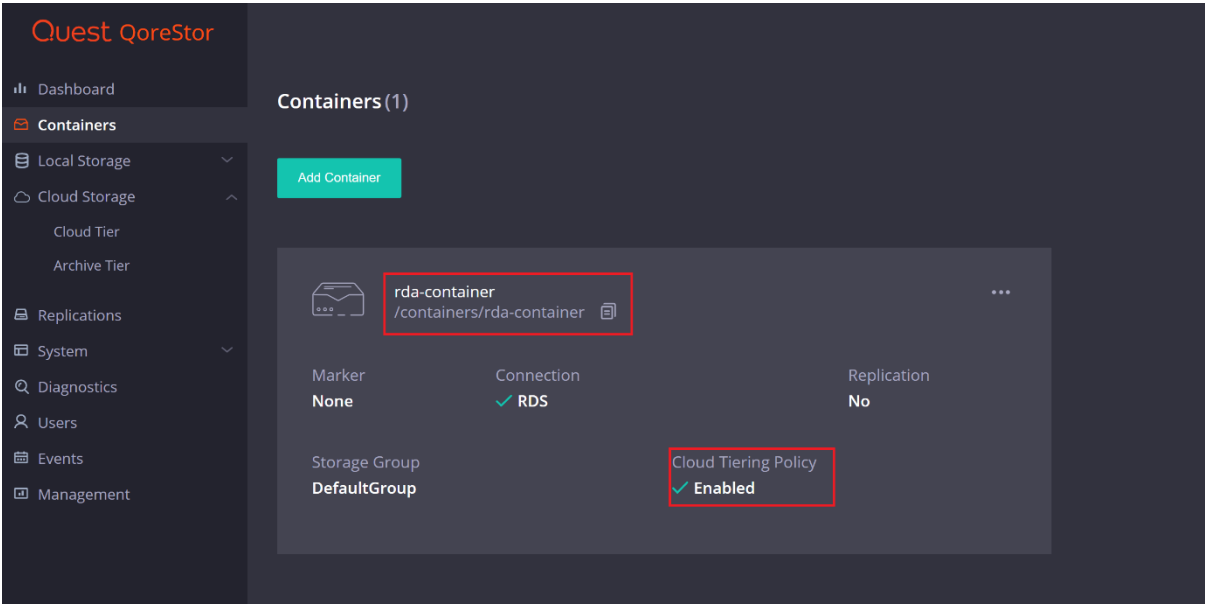
4. We need to add a cloud tiering policy to a specific container. Do this by navigating to the **Containers** page, selecting the **ellipsis** in the top right corner of the specific container, and clicking **Enabled Cloud Tiering Policy**.



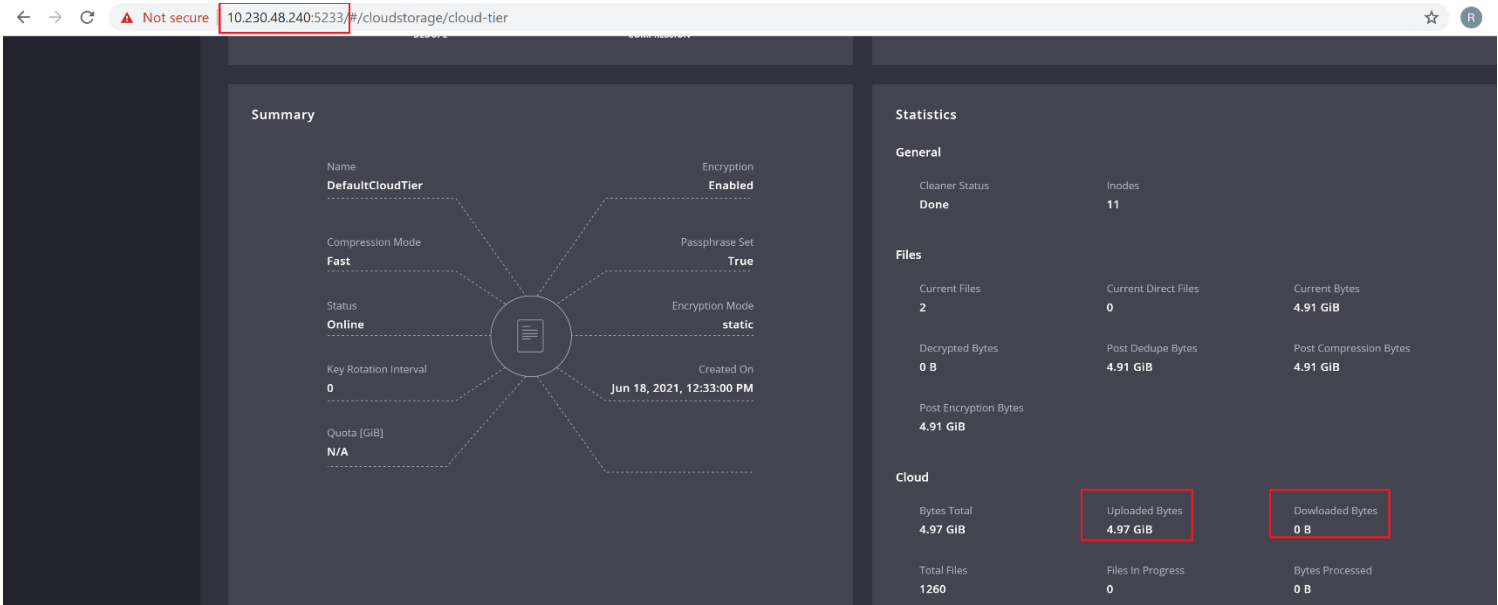
5. In the next window, we need to define the policy. **Idle time before cloud migration** specifies the number of hours/days datablocks must be kept idle before being sent to the cloud. **On-Prem Retention age** specifies the number of hours/days files will be kept locally after they are sent to the cloud. Finally, click **Enable**.



6. The container should now show with the cloud tiering policy enabled.



7. Verify the stats of cloud-uploaded bytes on the source QS machine after data gets replicated to the cloud from UI.



1. Verify the stats of cloud-uploaded bytes on the source QS machine after data gets replicated to the cloud from CLI.

```
[root@source-qs ~]# stats --cloud_tier
Storage_group ID      : 2
Total Inodes          : 11
Read Throughput       : 0.00 MiB/s
Write Throughput      : 0.00 MiB/s
Current Files         : 2
Current Direct Files  : 0
Current Bytes         : 5269335431
Post Dedupe Bytes     : 5269328759
Post Compression Bytes : 5269328759
Post Encryption Bytes  : 5271108000
Post Encryption Bytes in GiB : 4.9 GiB
Bytes decrypted       : 0
Cleaner Status        : Done
Compression Status    : Done
Encryption Status     : Pending
Dedupe Savings        : 0.00 %
Compression Savings    : 0.00 %
Total Savings         : 0.00 %
Cloud read Throughput : 0.00 MiB/s
Cloud write Throughput : 0.00 MiB/s
Files in progress to cloud : 0
Total cloud bytes uploaded : 5335719584
Total cloud bytes downloaded : 0
Total cloud cache bytes read : 0
Total cloud read bytes optimized: 0
Total cloud files     : 1260
Total cloud overwritten files : 0
Total cloud bytes     : 5335719584
Total cloud bytes processed : 0
Total cloud ds bytes reclaimed : 0
Total cloud metadata bytes : 64611584
Total space (rehydrated) : 5333947015
[root@source-qs ~]#
```



## 8. Cloud Reader

Once data gets replicated to the cloud, QoreStor allows it to read the data from the cloud to multiple target QS machines.

Note: During this time, all the target machines will be in cloud read-only mode. No writes are allowed from this reader QS to the cloud bucket whereas source QS continues to upload data to the same cloud bucket

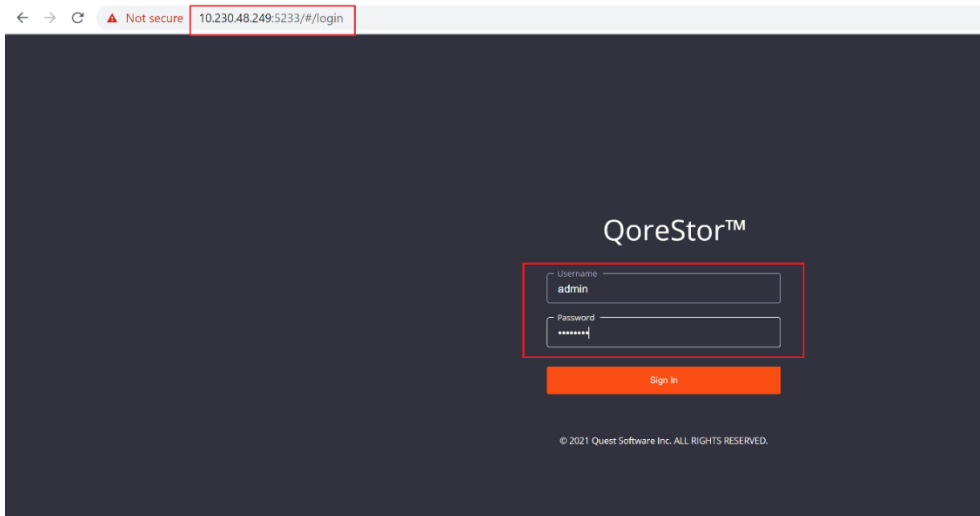
1. Log on to the QoreStor using SSH.

- a. Log in with username qsadmin.
- b. Run the following command on the target QoreStor machine to recover all the containers data:

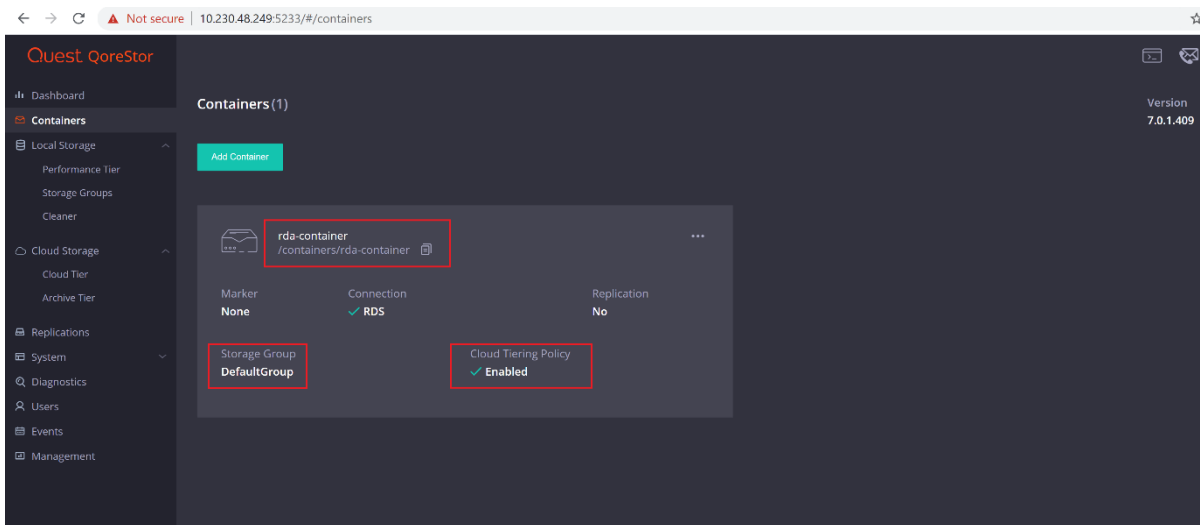
```
qsadmin@target-qs > maintenance --disaster_recovery --cloud_string
"DefaultEndpointsProtocol=https;AccountName=qorestortest;AccountKey=8Tt7/ysHSGSBSW7FG1Vr2+27xgccskbUWf9
GLIGEPeMHYfmVxl+fTg1XYpA==;EndpointSuffix=core.windows.net" --container_name cloud_container1 --
cloud_provider_type AZURE --passphrase qqg --logfile /tmp/t1 --quick_ro_recovery yes
Informing watcher to enter disaster recovery mode
Filesystem disaster recovery started successfully.
Please see the /var/log/oca/qsdr.log and the logfile given in the command.
qsadmin@target-qs >
```

--cloud_string	<azure connection string>
--container_name	<azure Cloud_container_name/bucketName>
--cloud_provider_type	AZURE
--passphrase	<Passphrase of cloud_tier> [set by the user while configuring cloudTier on source QS machine]
--logfile	</tmp/out6>
--quick_ro_recovery	< yes > will set target qorestor in read-only mode

2. Log in from UI on the target machine.



3. After logged-in, make sure the RDS container gets recovered.



4. From CLI, log in as qsadmin and verify the system state.

```
qsadmin@target-qs:~  
qsadmin@target-qs > system --show  
System Name : target-qs  
Current Time : Tue Jun 22 08:09:04 2021 EDT  
System ID : 42346F27C47C4361BB1EFDCA069B5B46  
Product Name : QoreStor  
Version : 7.0.1  
Build : 409  
Repository location : /ocareoot/ocareoot  
Metadata location : /ocareoot/qs_metadata  
Dictionary type : Standard  
System State : Operational Mode  
Reason : Filesystem is fully operational for I/O (Cloud access is read only)  
Configuration Server : RUNNING Jun 21 14:26:49  
Filesystem Server : RUNNING Jun 21 14:26:49  
Windows Access Server : RUNNING Jun 21 14:26:48  
Windows Active Directory Client : RUNNING Jun 21 14:26:09  
Health Monitor : RUNNING Jun 21 14:20:56  
Filesystem Checker : STOPPED  
SecureConnect Server : RUNNING Jun 21 14:26:48  
UI : RUNNING Jun 22 01:55:51  
Policy Manager Daemon : RUNNING Jun 21 14:28:13  
Disaster Recovery Daemon : STOPPED  
qsadmin@target-qs > █
```

5. Restore Data from the target QoreStor machine using BridgeHead :

- a. Run rdautil.exe on a BridgeHead Machine and Change the target QoreStor machine server address to restore from it

Note: Containers and storage groups are created with the same name. So, no need to change these details

```
c:\Htape\BN\cloud\rda>rdautil.exe
rdautil> set rda rdatarget1 /server=10.230.48.249

WARNING: You have requested access property change(s). Your
saved data may become inaccessible if these changes are
incorrect.

* Do you want to proceed? (Yes/No) : Yes

Proceeding...

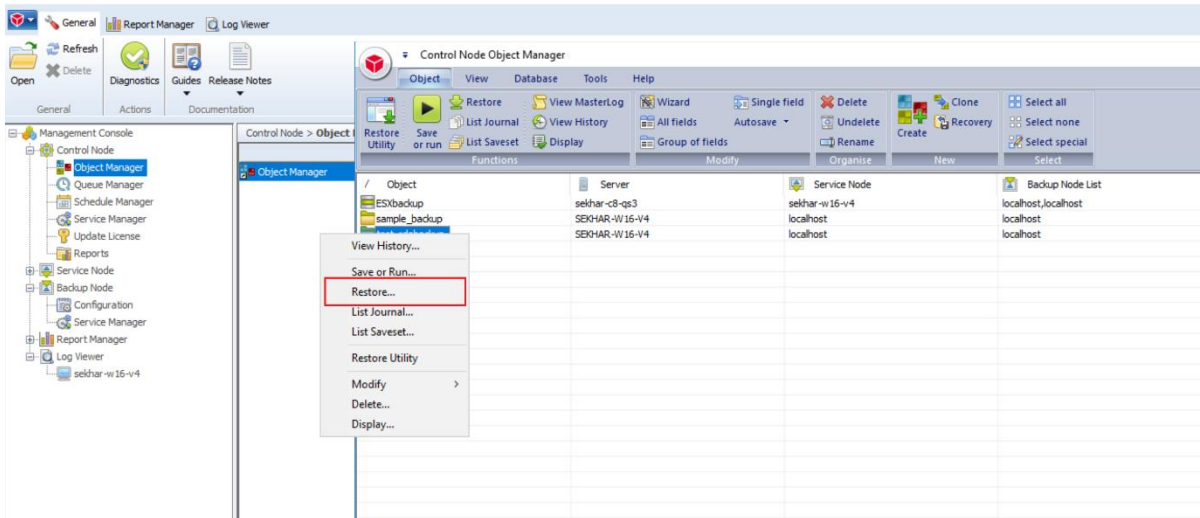
Instance attributes changed OK, new details are...

        Name: RDATARGET1
        Status: Initialized
        Server: 10.230.48.249
        Port: 0
        Username: backup_user
        Password: *****
        Container: rda-container
        Root directory: BridgeHead
        Write chunk size: 1024 KB
        Error limit: 5000
        Grace days: 5
        Secondary copy: (Blank)
        Tertiary copy: (Blank)
        Restore order: 123
        Daily job max concurrent jobs: 8
        Daily job progress check: 5 mins
        Daily job max replication time: 600 mins
        Daily job total run time: 900 mins
        Deduplication mode: Auto
        SecureConnect: On
        StorageGroup: DefaultGroup
        Logging: No
        Flags: 00000000 (=0 decimal)
        Comment: (Blank)

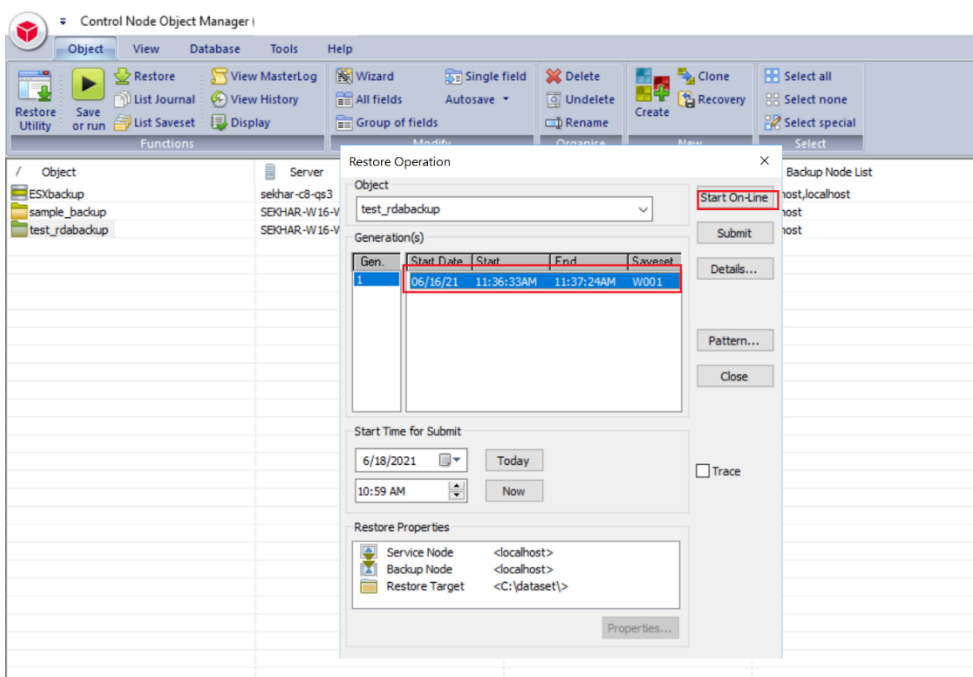
Updated marker object in RDA with new details.

rdautil> _
```

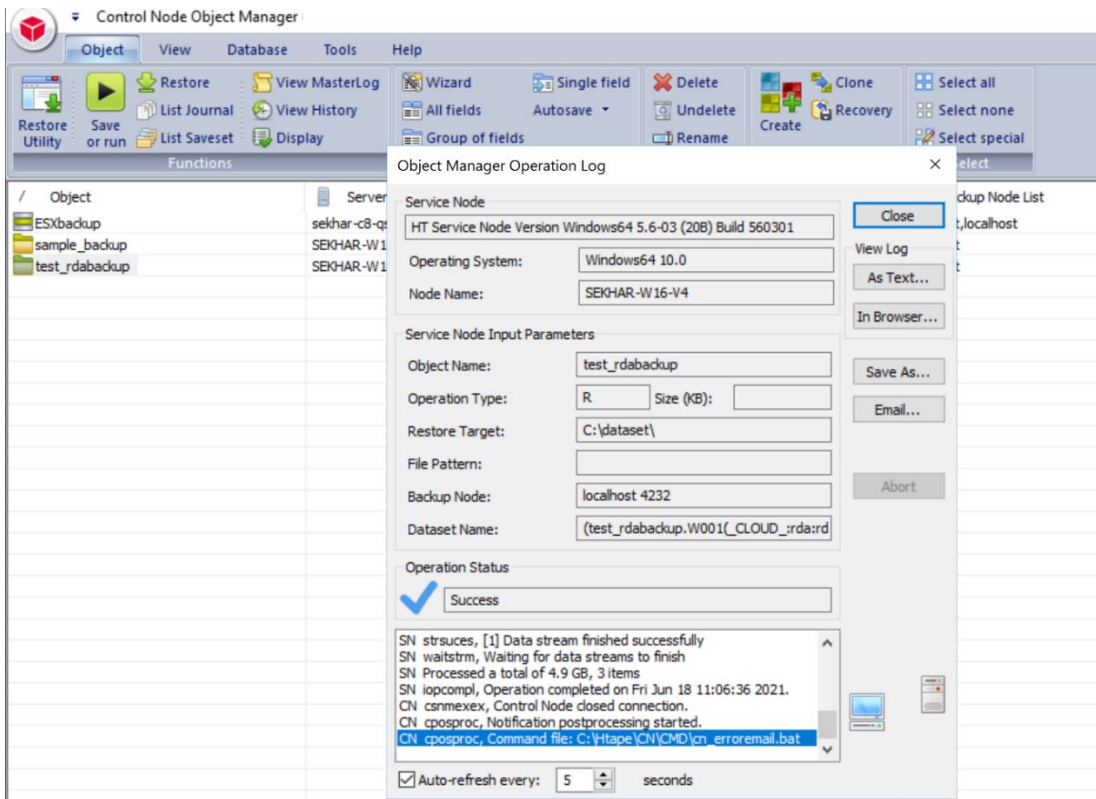
b. Open BridgeHead Management console, Now backup object summary is displayed on the Object list. Right-click the object to run the backup.



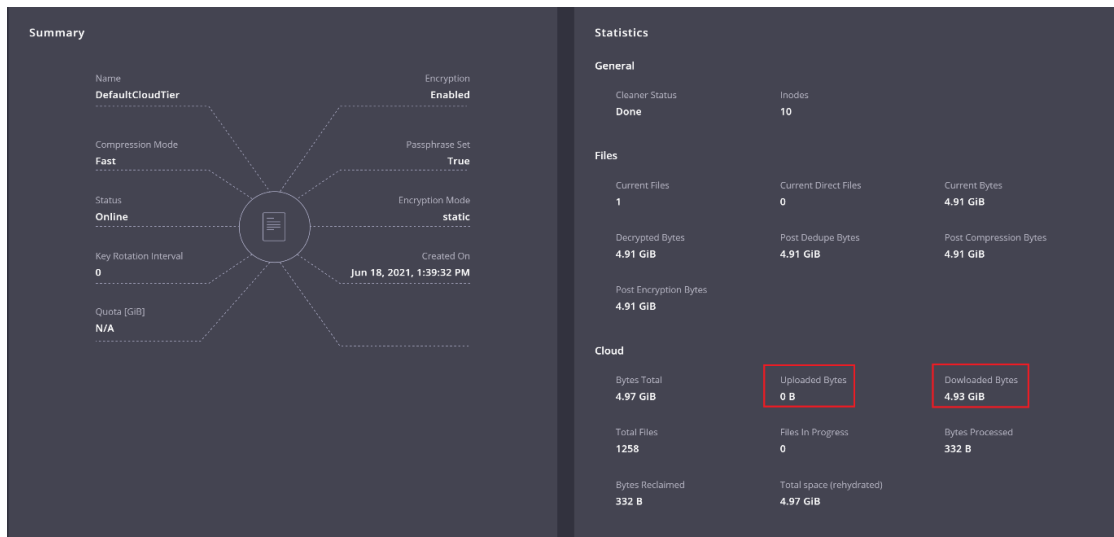
c. When the Restore window opens, click Start On-Line to start the restore.



d. The Object Manager Operation Log window displays the progress of the restore session. Operation status has details of the restore job.



e. Verify downloaded stats from the cloud on target qorestor.



f. Verify same from CLI

```
[root@test-qs ~]# stats --cloud_tier
Storage_group ID      : 2
Total Inodes          : 10
Read Throughput       : 0.00 MiB/s
Write Throughput      : 0.00 MiB/s
Current Files         : 1
Current Direct Files  : 0
Current Bytes         : 5269335099
Post Dedupe Bytes     : 5269328427
Post Compression Bytes : 5269328427
Post Encryption Bytes  : 5271107664
Post Encryption Bytes in GiB : 4.9 GiB
Bytes decrypted       : 5269335131
Cleaner Status        : Done
Compression Status    : Done
Encryption Status     : Pending
Dedupe Savings        : 0.00 %
Compression Savings   : 0.00 %
Total Savings         : 0.00 %
Cloud read Throughput : 0.00 MiB/s
Cloud write Throughput : 0.00 MiB/s
Files in progress to cloud : 0
Total cloud bytes uploaded : 0
Total cloud bytes downloaded : 5292088464
Total cloud cache bytes read : 271822412989
Total cloud read bytes optimized: 0
Total cloud files     : 1258
Total cloud overwritten files : 0
Total cloud bytes     : 5335604880
Total cloud bytes processed : 332
Total cloud ds bytes reclaimed : 332
Total cloud metadata bytes : 64497216
Total space (rehydrated) : 5333832315
[root@test-qs ~]#
```

## 9. Performance Tier

A Performance Tier allows you to define a set of faster disks as a Storage Group and created a container within that group. This Performance container will always read/write to these faster disks which will allow operations like restores and standard (non-fast clone) synthetic backups to occur quickly. This tier does not stage data off to the standard disks, this is because a restore of synthetic operation reading from the standard disks would still hamper the operation. All data written to the Performance Tier stays within the performance Tier. Because of this, it is recommended to write only specific jobs, which are required to be highly available and are sized to fit within the performance tier size. Please read the QoreStor User Guide for more details about the Performance Tier.



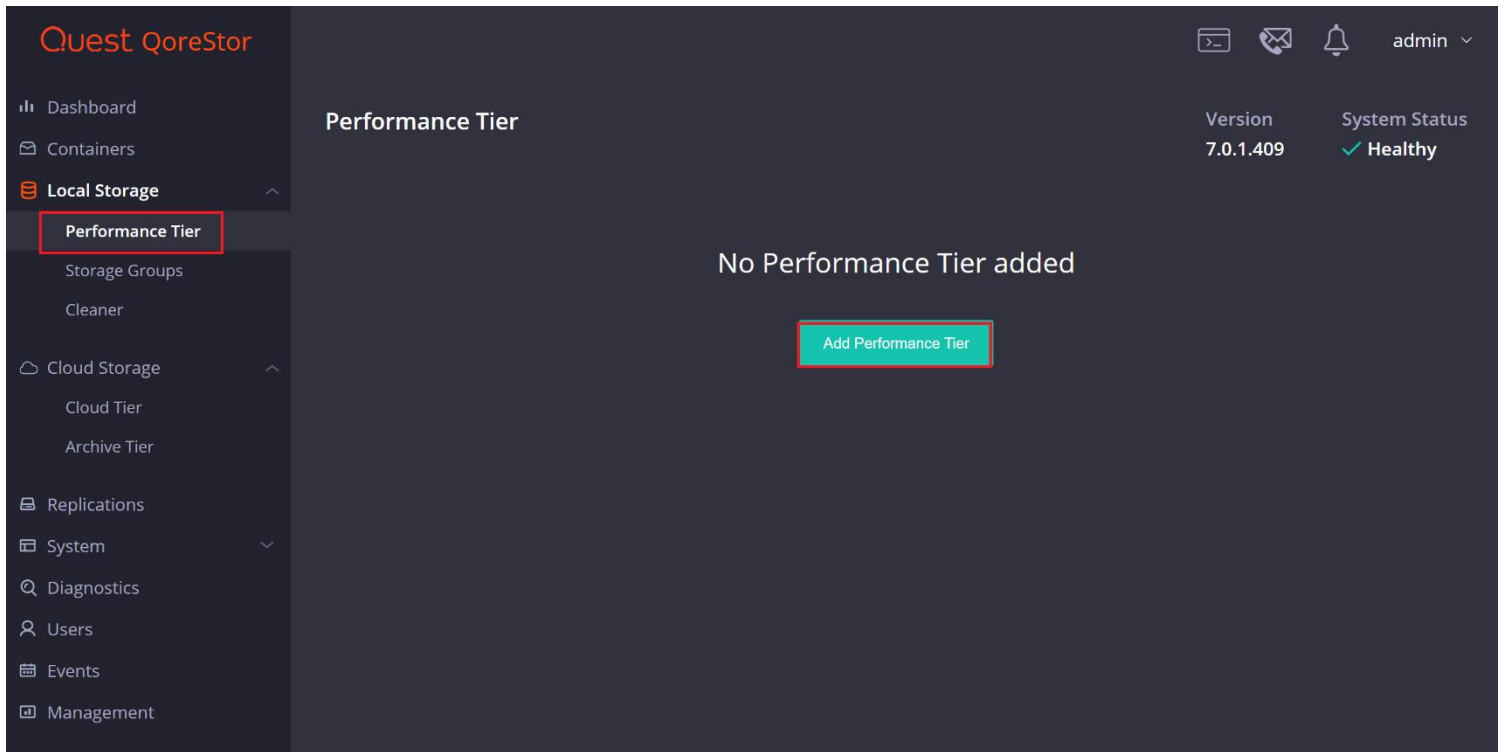
**Warning:** Please note that once a Performance Tier is added to a system it cannot be easily removed and attempting to do so will most likely result in the destruction of data. Please disable any backup or data copy jobs to the QoreStor system and contact support before attempting removal to find out if this is possible.

## Setting up Performance Tier with QoreStor

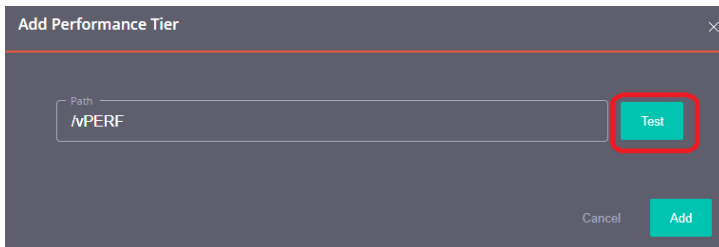
In this section, we are not going to cover adding a device, creating a partition, creating an XFS filesystem, or defining a mount point in detail. Please reference the QoreStor Installer Guide for this information.

- 1 We first need to cable and add the disks to the OS level. Once seen as a device in the OS an aligned partition will need to be created, an XFS file system created, and a mount point defined in fstab that includes mount option requirements defined in the QoreStor Installer guide.
2. Once a file system path to the high-performance storage is added the next step is to add that path as a performance tier in QoreStor. In the QoreStor UI expand **Local Storage** and select the **Performance Tier** tab. Click **Add Performance Tier**.

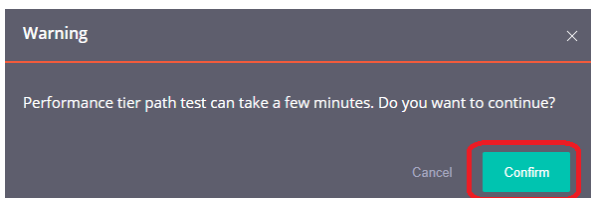




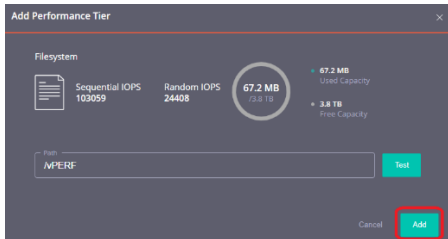
- 1 Enter the performance tier mount path and click the **Test** button.



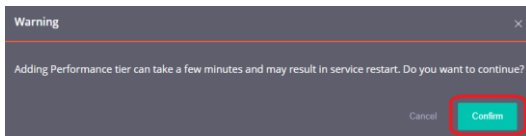
- 2 Click the **Confirm** button.



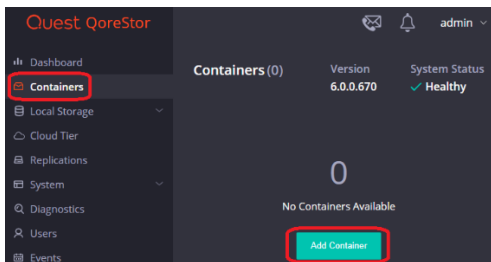
- 3 If the path gets the expected performance click **Add**.



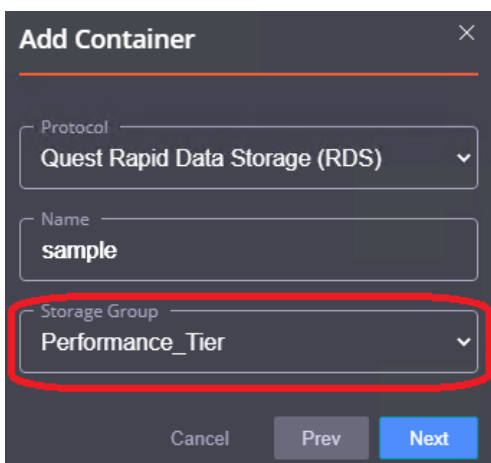
- 4 Click **Confirm** to finish adding the performance Tier, QoreStor services will be restarted.



- 5 Once the performance Tier is added you will be logged out. Once logged back in the Performance Tier tab will now list a dashboard for the performance Tier.
- 6 Navigate to the Containers tab and click Add Container.



8. In the **Storage Group** dropdown select **PerformanceTier**. Input the container **Name** and set the **Protocol** to **Quest Rapid Data Storage (RDS)**. Click **Next**.



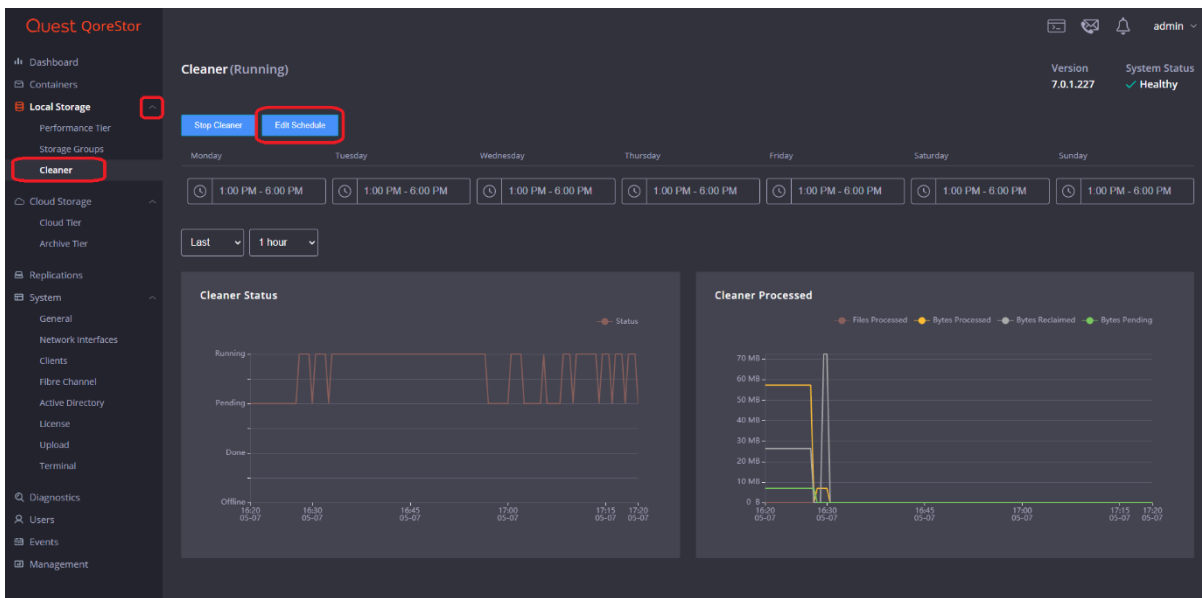
- Follow the rest of the steps listed in the **Creating an RDS container for BridgeHead** and **Adding an RDS container to BridgeHead** sections of this guide to finish configuring your Performance Tier container.

## 10. Setting up the QoreStor system cleaner

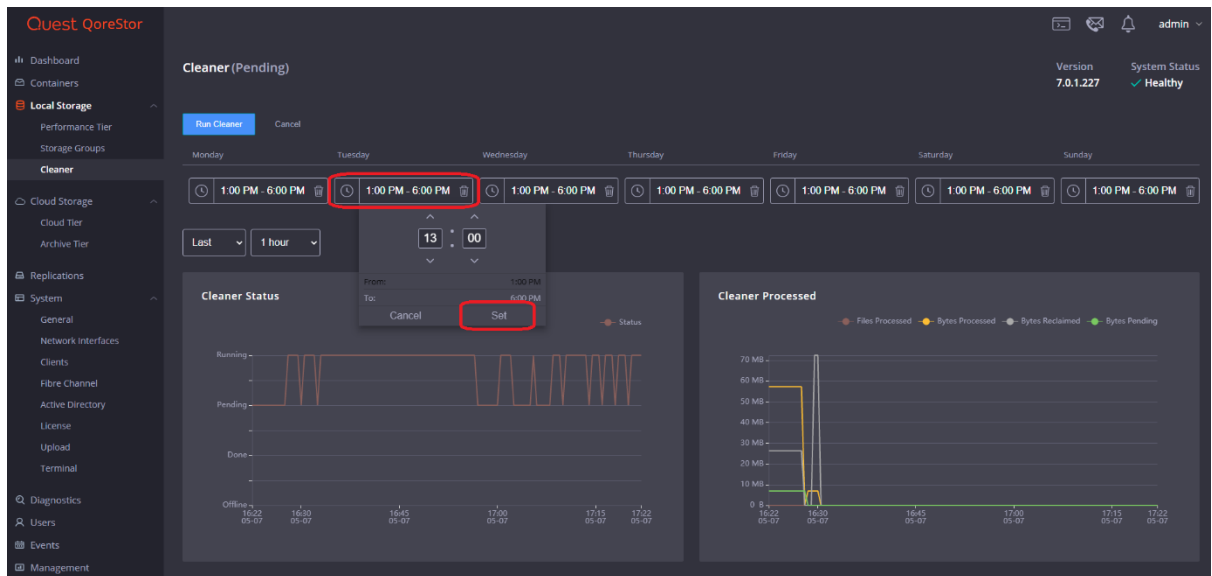
Performing scheduled disk space reclamation operations are needed as a method for recovering disk space from system containers in which files were deleted as a result of deduplication. Ideally, the QoreStor cleaner should complete a full cycle at least once a week. This will be accomplished in most cases by the predefined QoreStor cleaner schedule. The cleaner also runs during idle time.

To change the predefined cleaner schedule times, perform the following steps:

- Open the QoreStor administrative console.
- Expand **Local Storage** in the top navigation area.
- Select **Cleaner**.
- Click **Edit Schedule**.



5. Define the schedule and click **Set**.



If necessary, you can also perform a full cleaner cycle manually using either the QoreStor Administrative Console or QoreStor CLI.

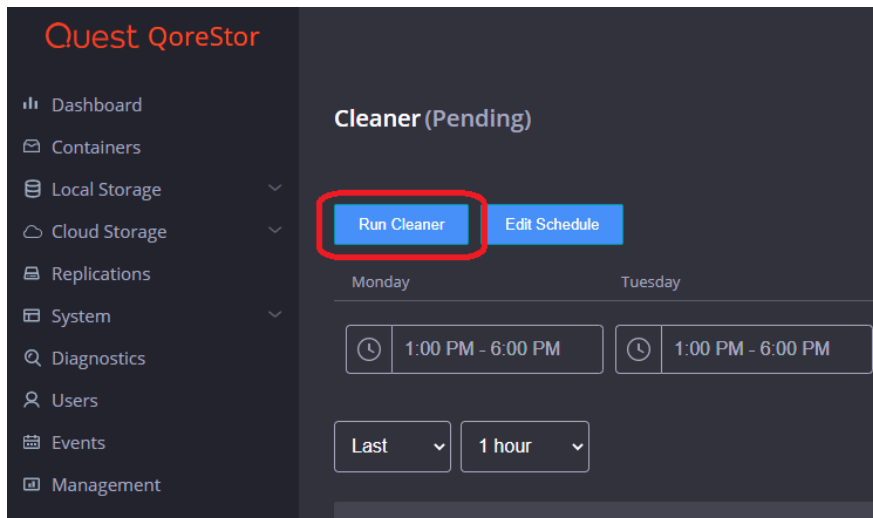
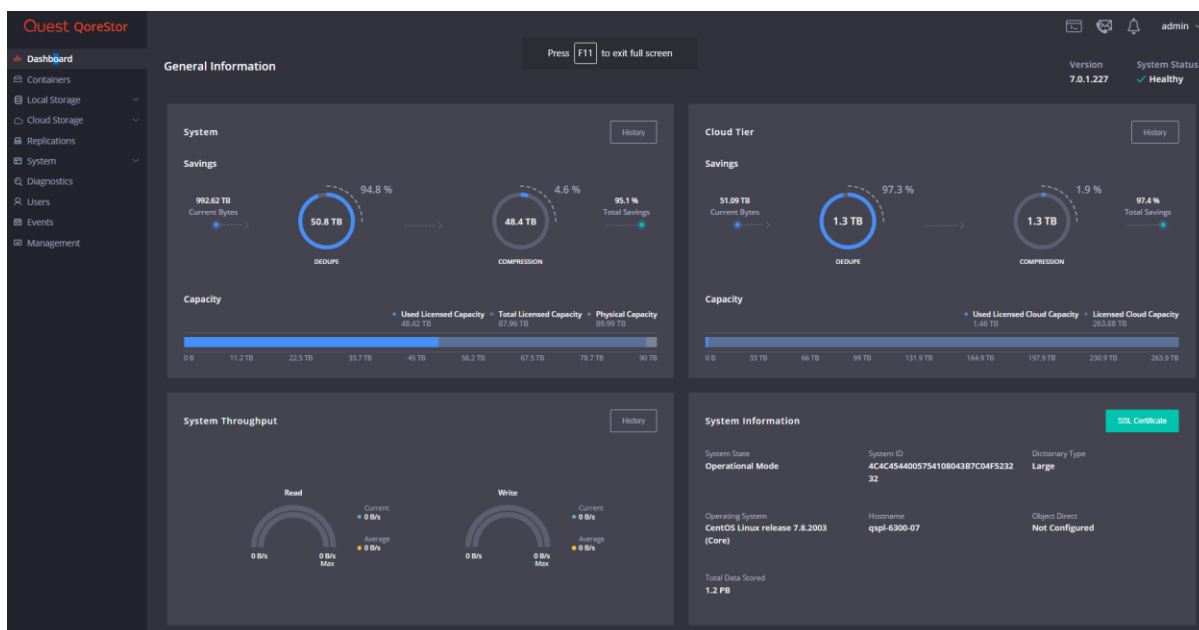


Figure 1: Using the QoreStor Administrative Console

```
# maintenance --filesystem --reclaim_space
# Successfully started cleaner.
```

## 11. Monitoring deduplication, compression, and performance

After backup jobs have run, the QoreStor system tracks capacity, storage savings, and throughput in the QoreStor dashboard. This information is valuable in understanding the benefits of the QoreStor software.



**i** **NOTE:** Deduplication ratios increase over time. It is not uncommon to see a 2-4x reduction (25-50% total savings) on the initial backup. As additional full backup jobs are completed, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio, in most cases.

# Appendix

## A. Create a Storage Device for CIFS

There are two options for BridgeHead HDM to authenticate to QoreStor through CIFS.

1. QoreStor is joined into an Active Directory Domain: Integrate BridgeHead HDM and QoreStor with Active Directory
  - a. Ensure the AD user has appropriate ACLs to the QoreStor Containershare
  - b. When creating an object, set the Backup Node of BridgeHead HDM to run with this AD user <DomainName\user>
2. QoreStor is a standalone CIFS server: Make sure this CIFS user has appropriate access permission to the QoreStor container share. BridgeHead HDM Backup Node will use this user to authenticate to QoreStor share in Workgroup mode.
  - a. To set the password for the local CIFS administrator on the QoreStor, log onto the QoreStor using SSH.
    - i. Log on with the username Administrator and password St0r@ge!
    - ii. Run the following command:  
Authenticate -- set -- user  
administrator

```
qsadmin@target-qs > authenticate --set --user administrator
Enter new password for CIFS user administrator:
Re-enter new password for CIFS user administrator:
Changed CIFS user "administrator" password.
qsadmin@target-qs > █
```

**Note:** The CIFS administrator account is a separate account from the administrator account used to administer the QoreStor. After an authentication method is chosen, set the BridgeHead Healthcare

## B. Create a Storage Device for NFS

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

1. Mount the QoreStor NFS share onto the NFS share directory which backup objects will be written in the BridgeHead Healthcare Data Management environment.
2. Verify the NFS share. One way is to try using the Linux command “cat /proc/mounts”. The rsize and wsize of the connect in the command output should be 512K.