

Module 5: Cloud Manager Features

Exercise 1: Protect Your Environment from Ransomware

In this exercise, you see how to protect your environment from ransomware by enabling Snapshot copy protection and blocking ransomware file extensions.

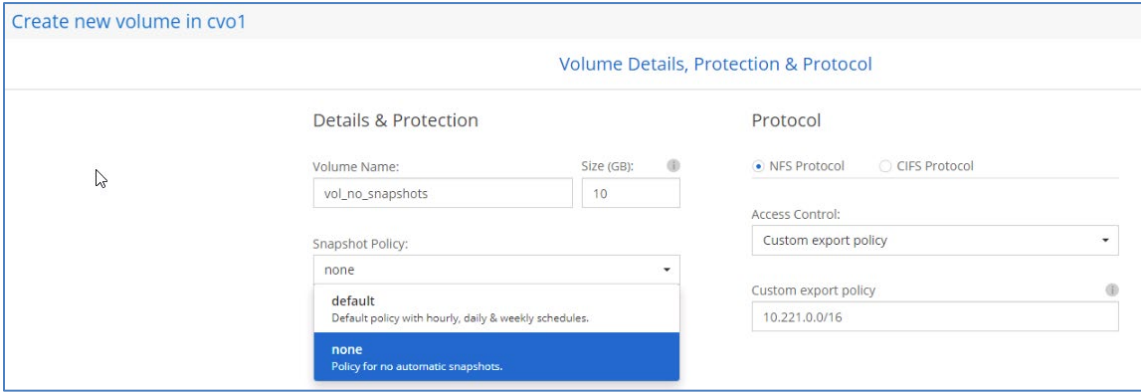
Objectives

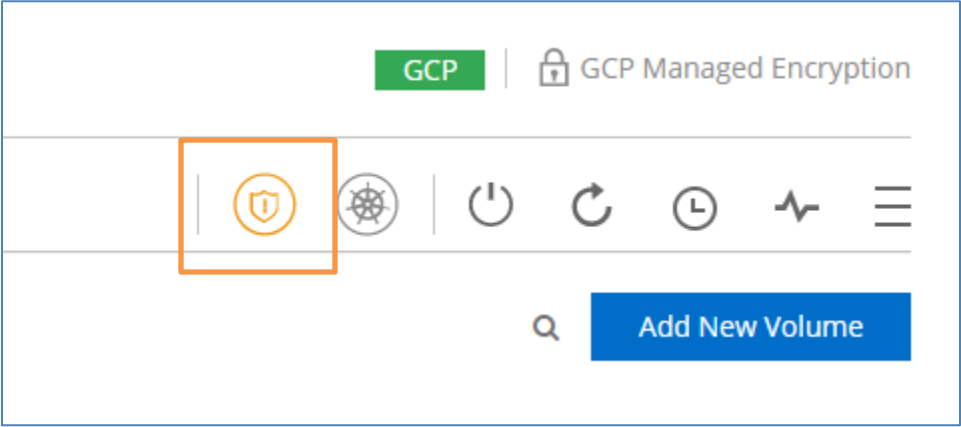
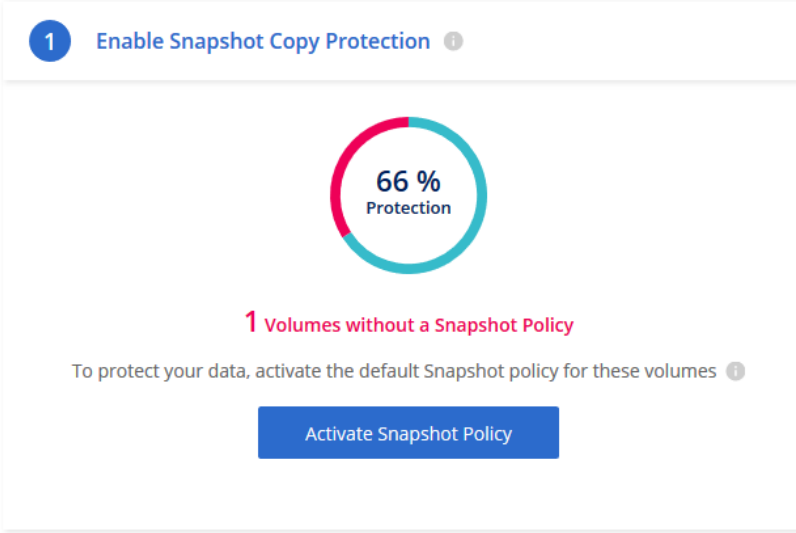
This exercise focuses on enabling you to do the following:

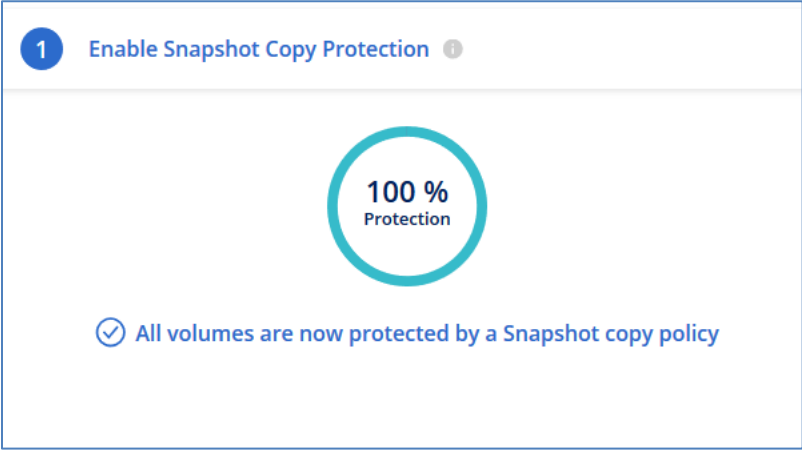
- Use Ransomware Protection tools to find missing Snapshot copy protection
- Block ransomware file extensions.

Task 1: Check for Missing Snapshot Copy Protection

In this task you create a volume without a snapshot policy and verify that the Ransomware protection tool finds the unprotected volume. You use the tool to activate snapshot for this volume.

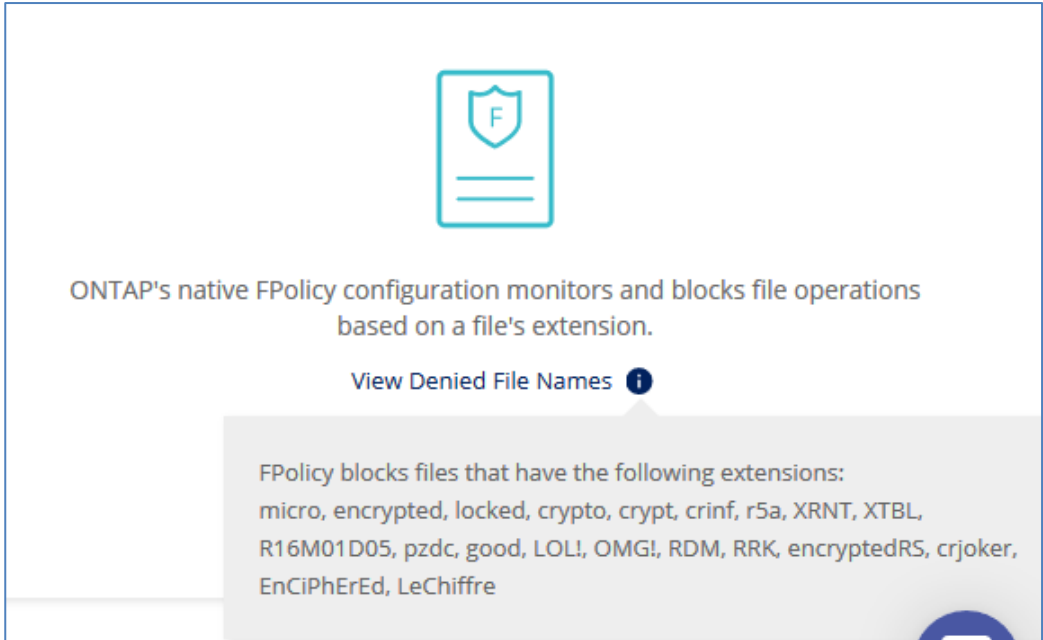
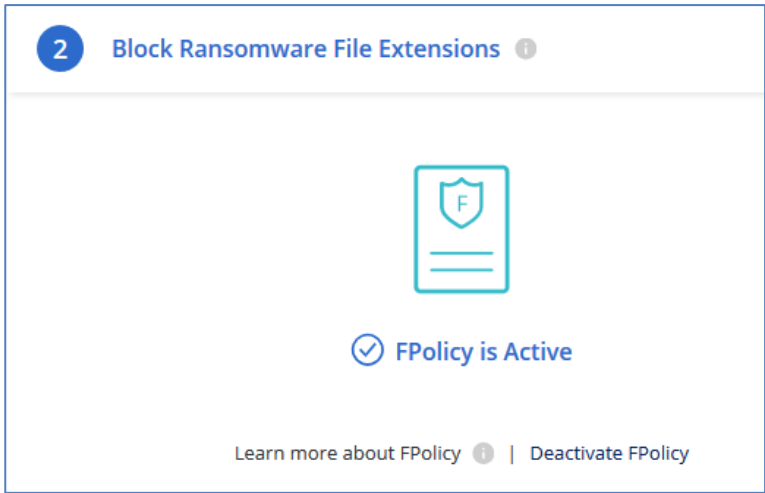
Step	Action
1-1	Return to Cloud Manager.
1-2	On the Volumes tab, click Add New Volume .
1-3	<div>On the Create new volume in cv01 page, enter the following:<ul style="list-style-type: none">• Volume Name: vol_no_snapshots• Size (GB): 10• Snapshot Policy: none</div>
1-4	Click Continue .
1-5	Click Go .

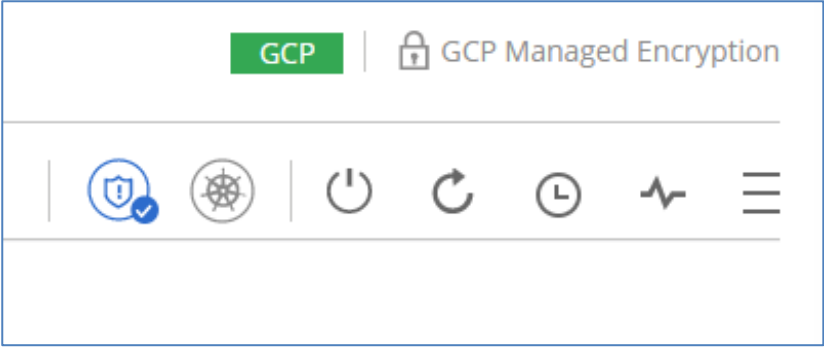
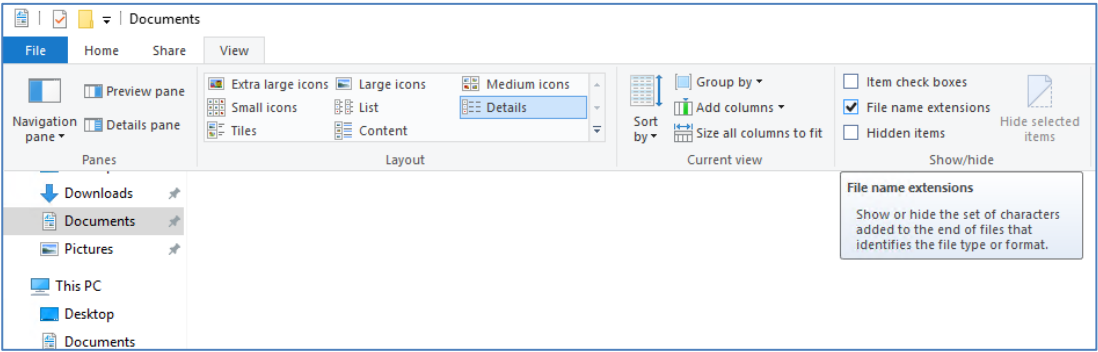
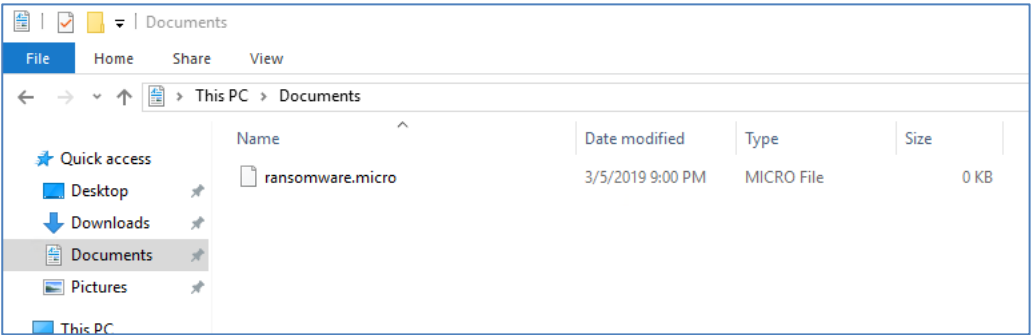
Step	Action
1-6	<p>On the Working Environment tool bar, click the Ransomware Protection icon.</p> 
1-7	<p>Verify that the Enable Snapshot Copy Protection finds one volume without a Snapshot policy.</p> <p>Ransomware Protection</p> <p>Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution</p> <p>1 Enable Snapshot Copy Protection</p> 
1-8	<p>Click Activate Snapshot Policy.</p>

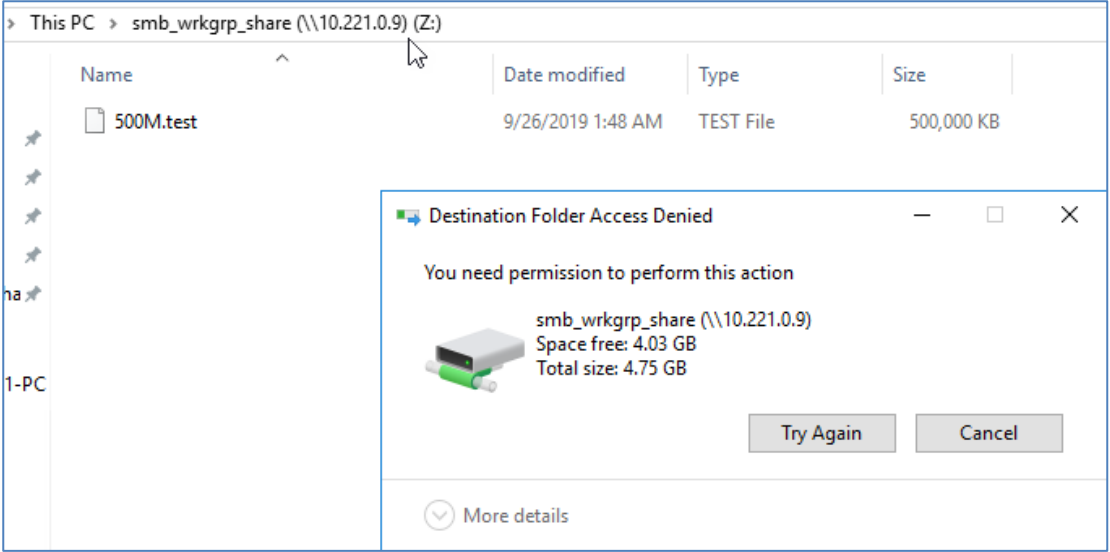
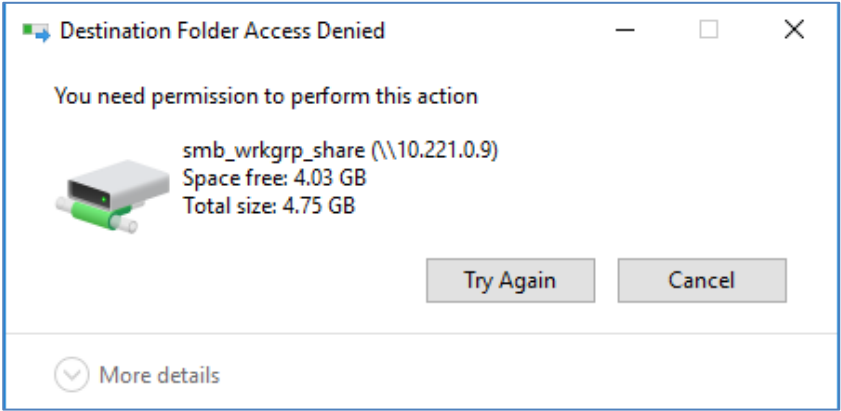
Step	Action
1-9	<p>Verify that your Snapshot copy protection is now 100%.</p>  <p>The screenshot shows a confirmation window with a teal circular progress indicator at 100%. Below the indicator, a checkmark icon is followed by the text 'All volumes are now protected by a Snapshot copy policy'. At the top left of the window, it says '1 Enable Snapshot Copy Protection' with an information icon.</p>
1-10	Delete the vol_no_snapshots volume.

Task 2: Block Ransomware File Extensions

In this task, you use the Ransomware protection tool to activate the FPolicy that blocks certain file extensions. You then verify that the tool blocks from writing a file with a .micro extension.

Step	Action
2-1	<p>Position your cursor over the info icon next to View Denied File Names, and review the file extensions that ONTAP's native FPolicy configuration blocks.</p> 
2-2	<p>Click Activate FPolicy.</p>
2-3	<p>Verify that the FPolicy is now active.</p> 

Step	Action
2-4	<p>You will also note that the Ransomware Protection icon is safe.</p> 
2-5	Return to the public-windows-instance.
2-6	Open File Explorer and go to the Documents folder.
2-7	<p>Click the View tab, and then select the File name extensions checkbox.</p> 
2-8	<p>Create a new text file called ransomware.txt, and then change the extension from .txt to .micro.</p> 

Step	Action
2-9	<p>Copy this file from the Documents folder to the smb_wrkgrp_share.</p> 
2-10	<p>Verify that you are unable to copy the file to the share.</p> 

End of Exercise