

## Exercise 3: Enabling Anti-Ransomware Protection

### Objectives

This exercise focuses on enabling you to do the following:

- Enable anti-ransomware protection in learning mode
- Activate anti-ransomware protection

### Case Study

Mr. Zarrot learns of ransomware attacks against industrial targets. He worries that Zarrot Industries might be at risk. He directs the IT staff to harden their defenses.

While other staff members ensure that the network firewall and anti-virus systems are in place and all systems are updated with the latest security patches, you enable the ONTAP ransomware detection and prevention features.

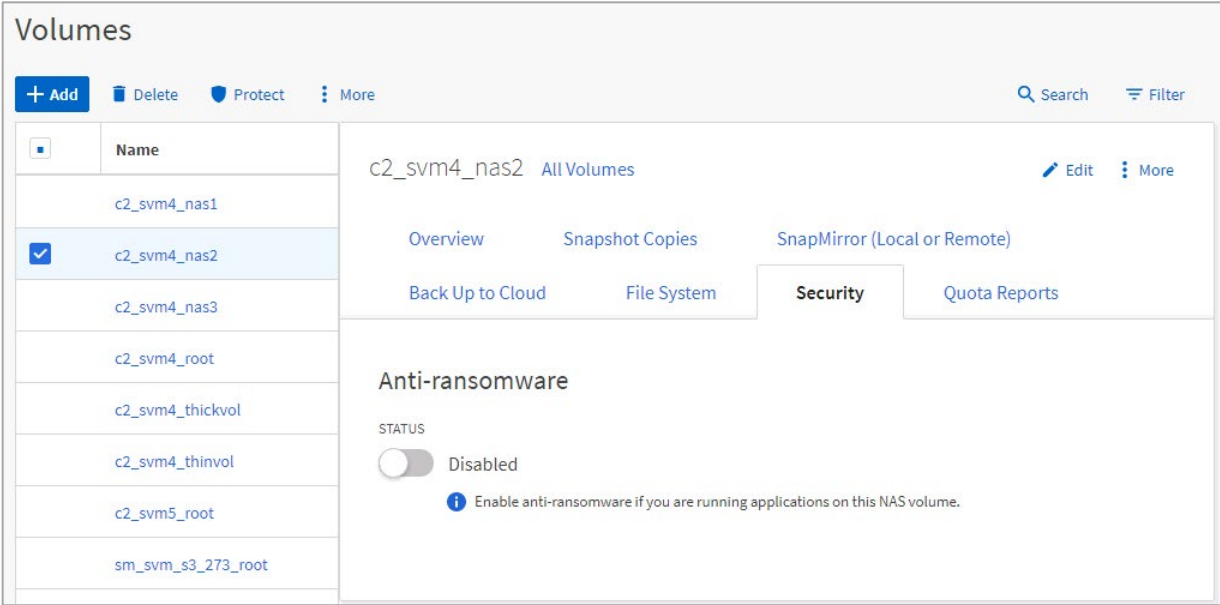
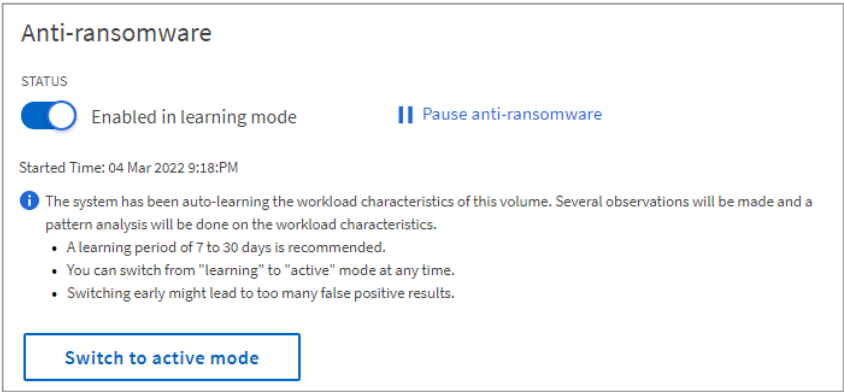
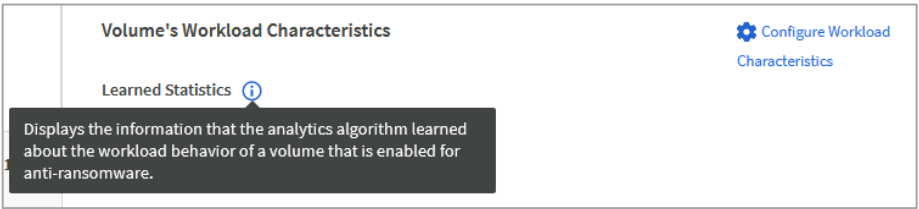
### Lab Equipment



Use the following equipment to complete the exercise:


| System                                  | Host Name | IP Addresses  | User Name              | Password |
|---|-----------|---------------|------------------------|----------|
| Windows Server                          | jumphost  | 192.168.0.5   | DEMO\Administrator     | Netapp1! |
| ONTAP cluster-management LIF (cluster2) | cluster2  | 192.168.0.102 | admin (case sensitive) | Netapp1! |

### Task 1: Enable Anti-Ransomware Protection

| Step | Action   |
|------|--|
| 1-1  | Log in to NetApp ONTAP System Manager for <b>cluster2</b> .        |
| 1-2  | From the System Manager menu, select <b>Storage &gt; Volumes</b> . |

| Step | Action   |
|------|--|
| 1-3  | <p>Select volume <b>c2_svm4_nas2</b>, and then click the <b>Security</b> tab.</p>  <p>The screenshot shows the 'Volumes' management interface. A list of volumes is on the left, with 'c2_svm4_nas2' selected. On the right, the 'Security' tab is active, displaying the 'Anti-ransomware' section where the status is currently 'Disabled'.</p>  |
| 1-4  | Click the Anti-ransomware <b>Status</b> toggle button to enable ransomware protection.   |
| 1-5  | <p>Observe the recommended learning period.</p>  <p>The screenshot shows the 'Anti-ransomware' status page. The status is 'Enabled in learning mode'. It includes a 'Switch to active mode' button and a list of recommendations for the learning period.</p>   |
| 1-6  | Scroll down the volume details page to the Volume's Workload Characteristics section.  |
| 1-7  | <p>Hover over the information icon to the right of Learned Statistics label, to learn about volume workload analysis.</p>  <p>The screenshot shows the 'Volume's Workload Characteristics' section. A tooltip is displayed over the 'Learned Statistics' label, explaining that it displays information about the analytics algorithm learned about the workload behavior of a volume that is enabled for anti-ransomware.</p> |
| 1-8  | Click <b>Configure Workload Characteristics</b> .  |

| Step | Action   |
|------|--|
| 1-9  | <p>Observe the types of activity that are monitored and the thresholds above which a snapshot copy is triggered.</p> <div data-bbox="240 233 1195 1146"> <h3>Configure Workload Characteristics</h3> <p>The following workload characteristics are used to detect ransomware attacks.<br/>When a surge is detected that is higher than the set expectation, a Snapshot copy is created. <a href="#">Know more</a></p> <p><input checked="" type="checkbox"/> Monitor surges in high entropy data <a href="#">?</a></p> <p>MAXIMUM RATE IN HIGH ENTROPY DATA THAT IS CONSIDERED NORMAL</p> <p>100 %</p> <p><input checked="" type="checkbox"/> Monitor surges in file create operations</p> <p>MAXIMUM RATE OF CREATE OPERATIONS THAT IS CONSIDERED NORMAL</p> <p>100 %</p> <p><input checked="" type="checkbox"/> Monitor surges in file delete operations</p> <p>MAXIMUM RATE OF DELETE OPERATIONS THAT IS CONSIDERED NORMAL</p> <p>100 %</p> <p><input checked="" type="checkbox"/> Monitor surges in file rename operations</p> <p>MAXIMUM RATE OF FILE RENAME OPERATIONS THAT IS CONSIDERED NORMAL</p> <p>100 %</p> </div> |
| 1-10 | <p> After ONTAP software has had sufficient time to monitor volume file I/O activity and learn normal behavior, you can use the learned statistics to adjust the Snapshot copy trigger thresholds.</p>  |
| 1-11 | Click <b>Cancel</b> .  |
| 1-12 | <p>Switch the anti-ransomware protection to active mode.</p> <div data-bbox="240 1417 1075 1803"> <h3>Anti-ransomware</h3> <p>STATUS</p> <p><input checked="" type="checkbox"/> Enabled in learning mode <a href="#">Pause anti-ransomware</a></p> <p>Started Time: 04 Mar 2022 9:18:PM</p> <p> The system has been auto-learning the workload characteristics of this volume. Several observations will be made and a pattern analysis will be done on the workload characteristics.</p> <ul style="list-style-type: none"> <li>• A learning period of 7 to 30 days is recommended.</li> <li>• You can switch from "learning" to "active" mode at any time.</li> <li>• Switching early might lead to too many false positive results.</li> </ul> <p><a href="#">Switch to active mode</a></p> </div>   |

| Step | Action   |
|------|--|
| 1-13 | <div data-bbox="240 153 337 247">  </div> <p data-bbox="362 153 1425 254">ONTAP software requires time to learn normal file I/O activity before it can identify abnormal activity that might indicate a ransomware attack. There is not adequate time in this course to demonstrate ONTAP software detecting a simulated attack.</p> <p data-bbox="240 268 1466 338">To learn more about ONTAP ransomware protection and to practice responding to a ransomware attack, see the <i>ONTAP Security and Compliance Solutions Administration</i> course.</p> |

**End of exercise**