7 - Volume Shadow Copy Service

Task 9 ✅ Volume Shadow Copy Service

Per Microsoft, the **Volume Shadow Copy Service** (VSS) coordinates the required actions to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.

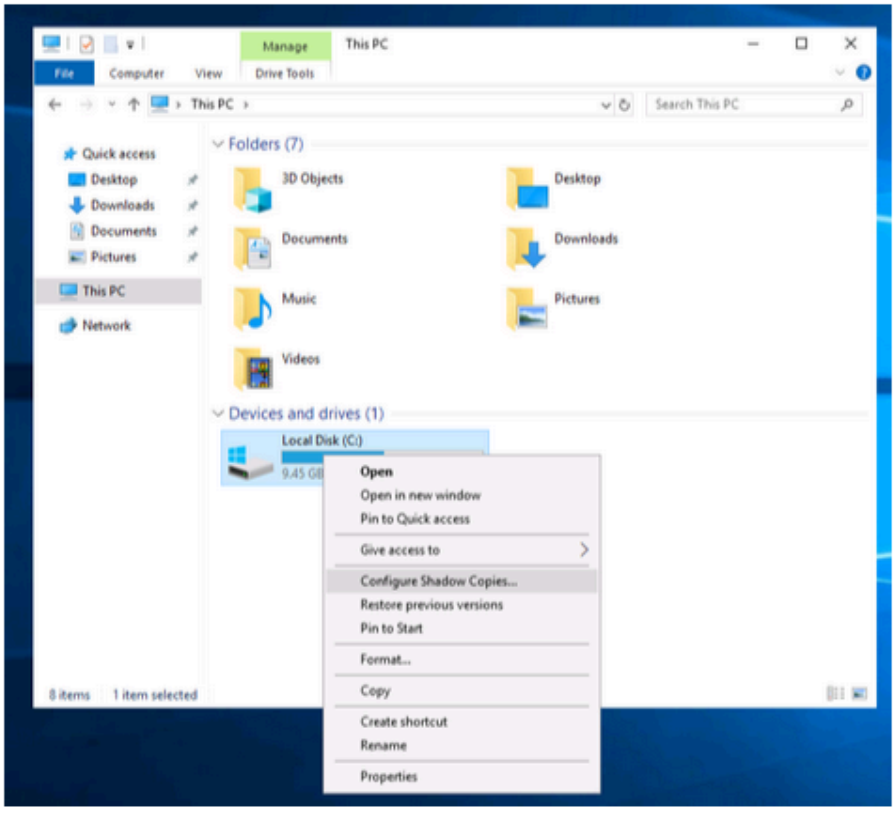
Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.

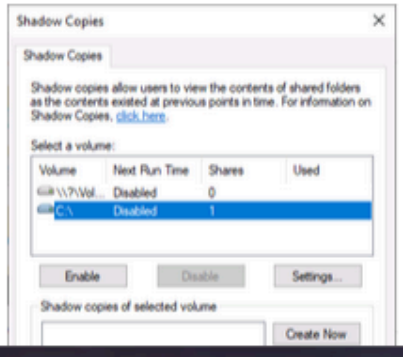
If VSS is enabled (**System Protection** turned on), you can perform the following tasks from within **advanced system settings**.

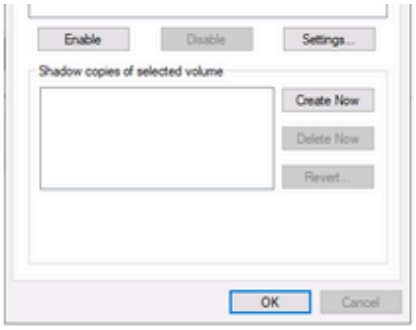
- **Create a restore point**
- **Perform system restore**
- **Configure restore settings**
- **Delete restore points**

From a security perspective, malware writers know of this Windows feature and write code in their malware to look for these files and delete them. Doing so makes it impossible to recover from a ransomware attack unless you have an offline/off-site backup.

If you wish to configure Shadow Copies within the attached VM, see below.







Bonus: If you wish to interact hands-on with VSS, I suggest exploring Day 23 of Advent of Cyber 2.

Answer the questions below

What is VSS?

Volume Shadow Copy Service ✓ Correct Answer

Task 10 Conclusion

In this room, we covered several built-in Windows security tools that ship with the Windows OS to help keep the device protected.

There is still so much to explain and cover regarding the Windows OS. As mentioned in the Windows Fundamentals 1 room, "*The content is aimed at those who wish to understand and use the Windows OS on a more comfortable level*."

To learn more about the Windows OS, you'll need to continue the journey on your own.

Further reading material:

- Antimalware Scan Interface
- Credential Guard
- Windows 10 Hello
- CSO Online - The best new Windows 10 security features

Note: Attackers use built-in Windows tools and utilities in an attempt to go undetected within the victim environment. This tactic is known as Living Off The Land. Refer to the following resource here to learn more about this.

Answer the questions below

Read the above.

No answer needed Complete