

### **Assignment 3: Disk Management and File/folder Systems and Security**

Alexander M. Hendren

Nova Scotia Community College, Cyber Security

OSYS1020

Russell Munday

October 25, 2024

## **Table of Contents**

<b>Section 1: Document Introduction .....</b>	<b>3</b>
<b>Section 2: Adding Disk Management to Security Console and Setting Up Drives .....</b>	<b>4</b>
<b>Section 3: Creating New Folders .....</b>	<b>5</b>
<b>Section 4: Reviewing Encryption Certificate .....</b>	<b>6</b>
<b>Section 5: Adding Security Groups .....</b>	<b>7</b>
<b>Section 6: Design and Implement a Folder Structure .....</b>	<b>8</b>
<b>Section 7: Backup and PostA3 Snapshot .....</b>	<b>9</b>

## **Section 1: Document Introduction**

This Assignment teaches us how to add additional drives and create different RAID configurations, change folder permissions, encrypt and compress folders and implements an NTFS folder structure in our Windows 10 Virtual Machine. From reading this document, the reader will be walked through the steps listed above, using screenshots and a ICALCS report.

## Section 2: Adding Disk Management to Security Console and Setting Up Drives

In this section, we will be using Disk Management to setup our additional disks that will be used for this assignment. To do this we open MMC and click “add a snap in” we then find Disk Management and add it. We then assign drive letter E to our 10g drive, we format it with NTFS and give it the label “Company Data” and perform a quick format. We then do the same with our 20g disk and assign drive letter F and volume label “Data”. We then restart our machine to let the changes take place.

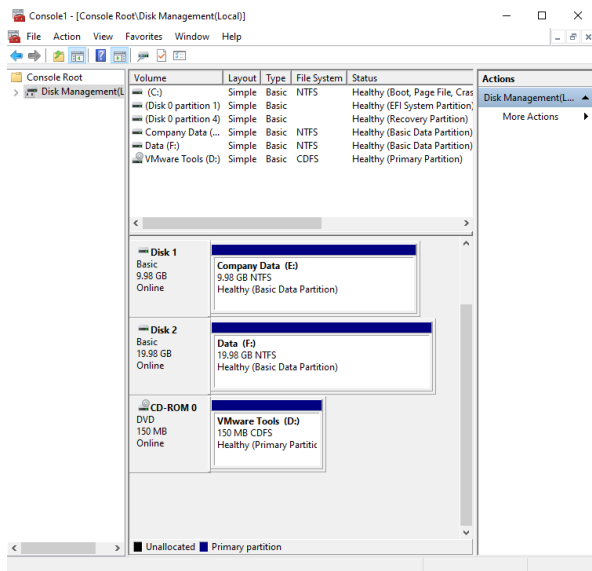


Image 1. Disk Management snap-in

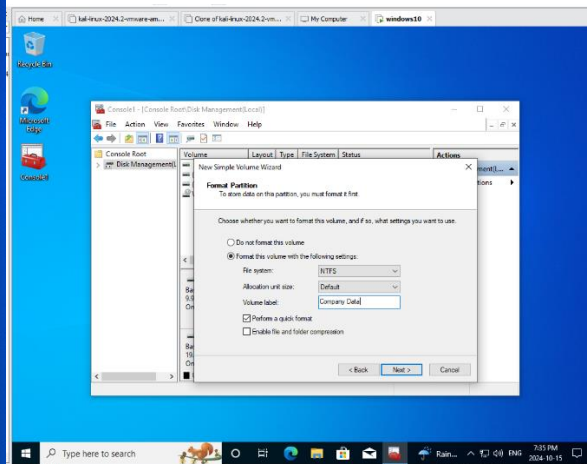


Image 2. Formatting Drives

The screenshots above show we have added device management and formatted our 10g and 20g disks.

## Section 3: Creating New Folders

In this section, we will be creating a folder structure. We will be creating a compressed folder C and file C on drive F, and an encrypted folder E and file E on the drive F. We will also be downloading our encryption certificate. To do this we will create “FolderC” on the root of the F drive, we then compress the folder and create a “FileC” inside.

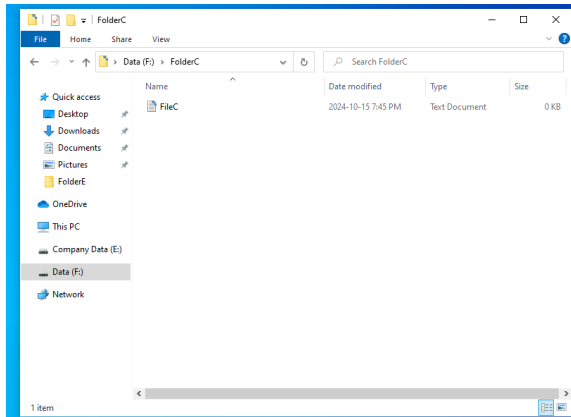


Image 3. File C and Folder C

Next, we create a new folder titled folder “E”. Using the NTFS Encrypt Attribute we can encrypt this folder. After the folder is encrypted, we use the Certificate Export Wizard to backup our keys. We use the default file format and settings, and we use the encryption type TripleDES-SHA1. After this is done, we create an encrypted file inside of folder “E” titled File “E”.

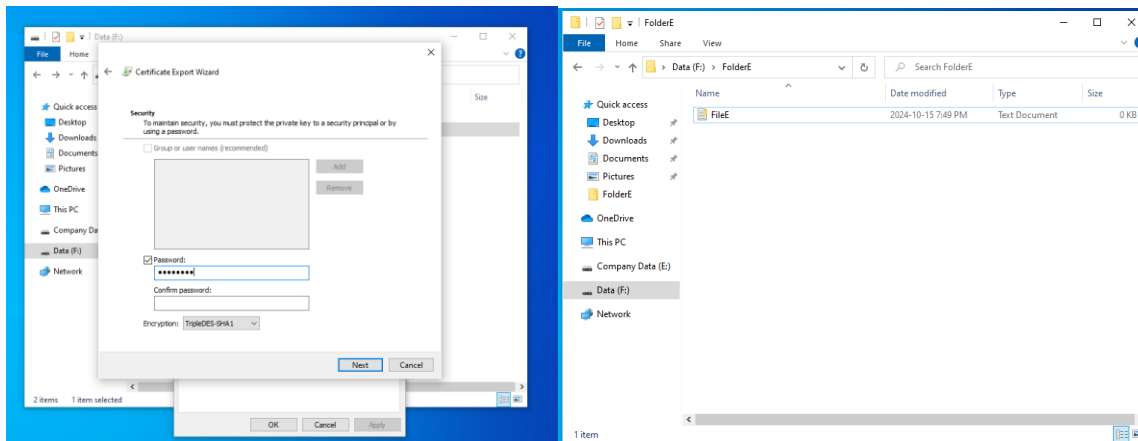
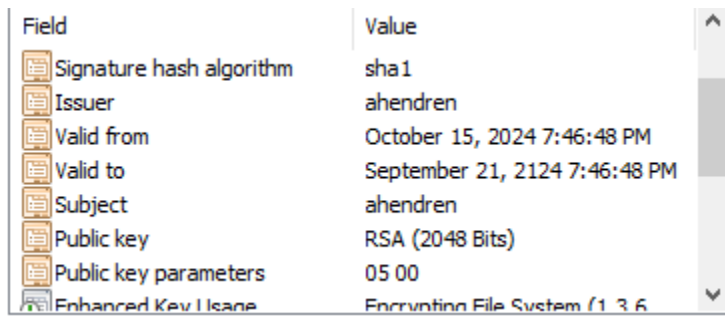


Image 4. Certificate Export Wizard

Image 5. File E and Folder E

## Section 4: Reviewing Encryption Certificate

In this section, now that we have our encryption certificate, we will review what is stored on it. To do this we open MMC and add the certificates snap-in. We find the certificate we created and edit it to the proper names. After this review the properties of the certificate to see when it was issued, who it was issued to, the hash algorithm, the issuer, the public key and the certificate path.



Field	Value
Signature hash algorithm	sha1
Issuer	ahendren
Valid from	October 15, 2024 7:46:48 PM
Valid to	September 21, 2124 7:46:48 PM
Subject	ahendren
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Encryption File System (1.3.6

Image 6. Certificate Properties

## Section 5: Adding Security Groups

In this section, we will be creating security groups. To do this we will open console.msc and select groups. We will create 3 new groups and add descriptions, these groups are Sales, Marketing and Management.



Image 7. Creating Groups

## Section 6: Design and Implement a Folder Structure

In this section we will be designing and implementing a folder structure. To do this we will create a new folder called “CompanyInc”. We will create a subfolder for each group we made in the last section. Now we must set permissions for the subfolders. We copy the permission parameters from the instructions in the assignment. After this is done, we must run the command “ICACLS E:\CompanyInc\ /T >> C:\Reports\ACLReports.txt”. This will generate an ACL report, which is attached to my Brightspace submission.

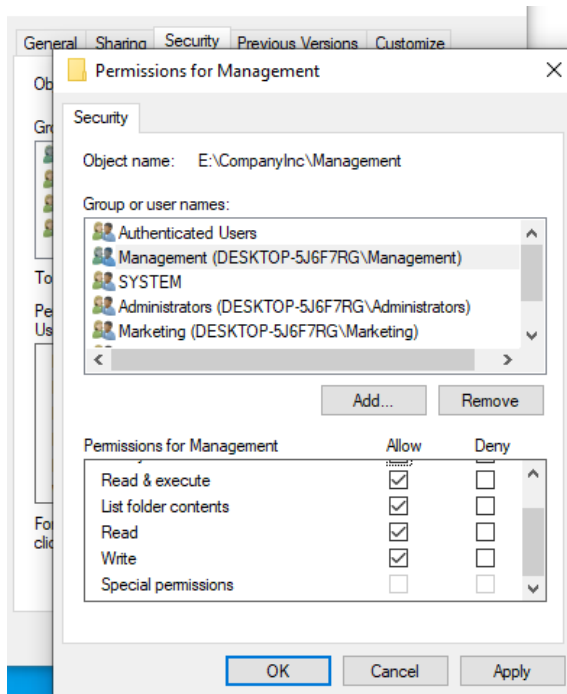


Image 8. Setting Permissions



## Section 7: Backup and PostA3 Snapshot

In this section, we must backup our VM and crate a new snapshot. To do this we will make a new copy of our VM, and a new snapshot titled “PostA3”.

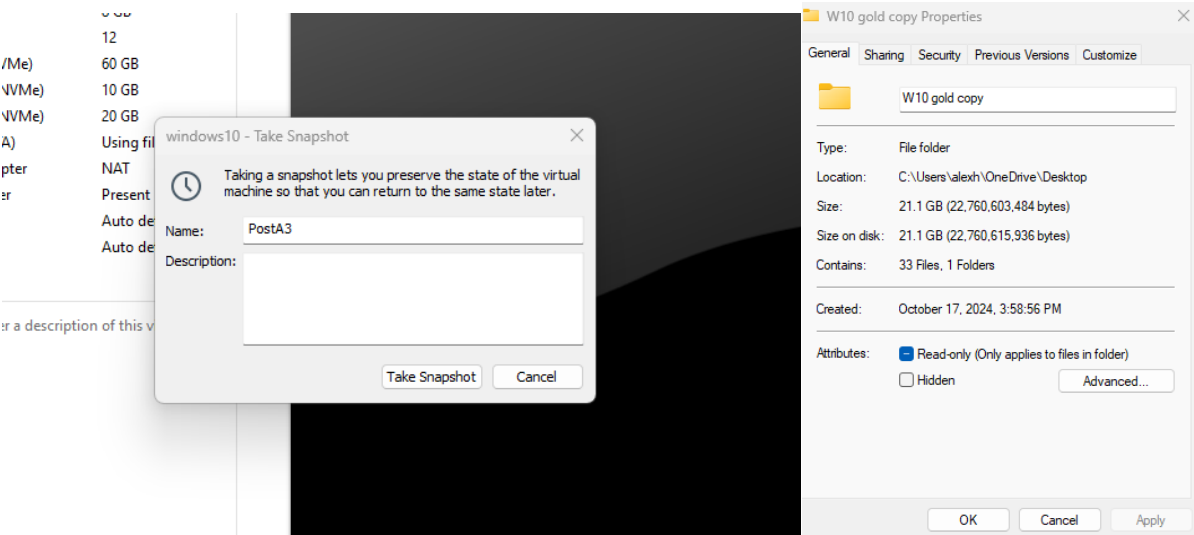


Image 10. PostA3 Snapshot Created

Image 9. Gold Copy Created