

IT 236 Project Report Form

Report Prepared By:	Vivian J. Goshashy
Date:	11/05/2025
Project Phase	Configuring Storage Replica for Data Resiliency

Section 1: Executive Summary (20 points)

This report presents the implementation and validation of Storage Replica between NV-FS1 and NV-DC1 as part of the ongoing NewVue Health Infrastructure Modernization Project. The goal of this phase was to ensure data resiliency, business continuity, and high availability across the network infrastructure.

Through the successful deployment of Storage Replica, the organization now maintains a continuously updated copy of departmental data hosted on NV-FS1. This redundancy minimizes downtime and protects critical files in the event of hardware or service failure. The configuration also established secure management communication between servers through WinRM over HTTPS, using self-signed certificates and mutual trust validation.

Verification steps confirmed healthy replication, switch-direction functionality, and read-only access to data during simulated source server failure.

Replication Configuration Summary

Server	Role	Data Volume	Log Volume	Replication Direction
NV-FS1	Source	NewVueData (E:\)	New Volume (F:\)	Send
NV-DC1	Destination	DC1_Data (E:\)	New Volume (F:\)	Receive

Scope of Work

The activity included:

- Installing and validating the Storage Replica feature on both NV-FS1 and NV-DC1.
- Preparing and configuring dedicated data (E:) and log (F:) volumes on both servers to host the replicated file shares and replication metadata.\
- Securing server management channels by configuring WinRM over HTTPS and establishing mutual certificate trust between NV-FS1 and NV-DC1.

- Deploying Windows Admin Center on NV-FS1 to provide a centralized management dashboard for the replication partnership.
- Creating and configuring a synchronous replication partnership, designating NV-FS1 as the source and NV-DC1 as the destination.
- Thoroughly monitoring replication health, validating data synchronization, and conducting a failure simulation to confirm business continuity processes, including switch-over and read-only access to the replicated data.

Section 2: Implementation and Verification Evidence

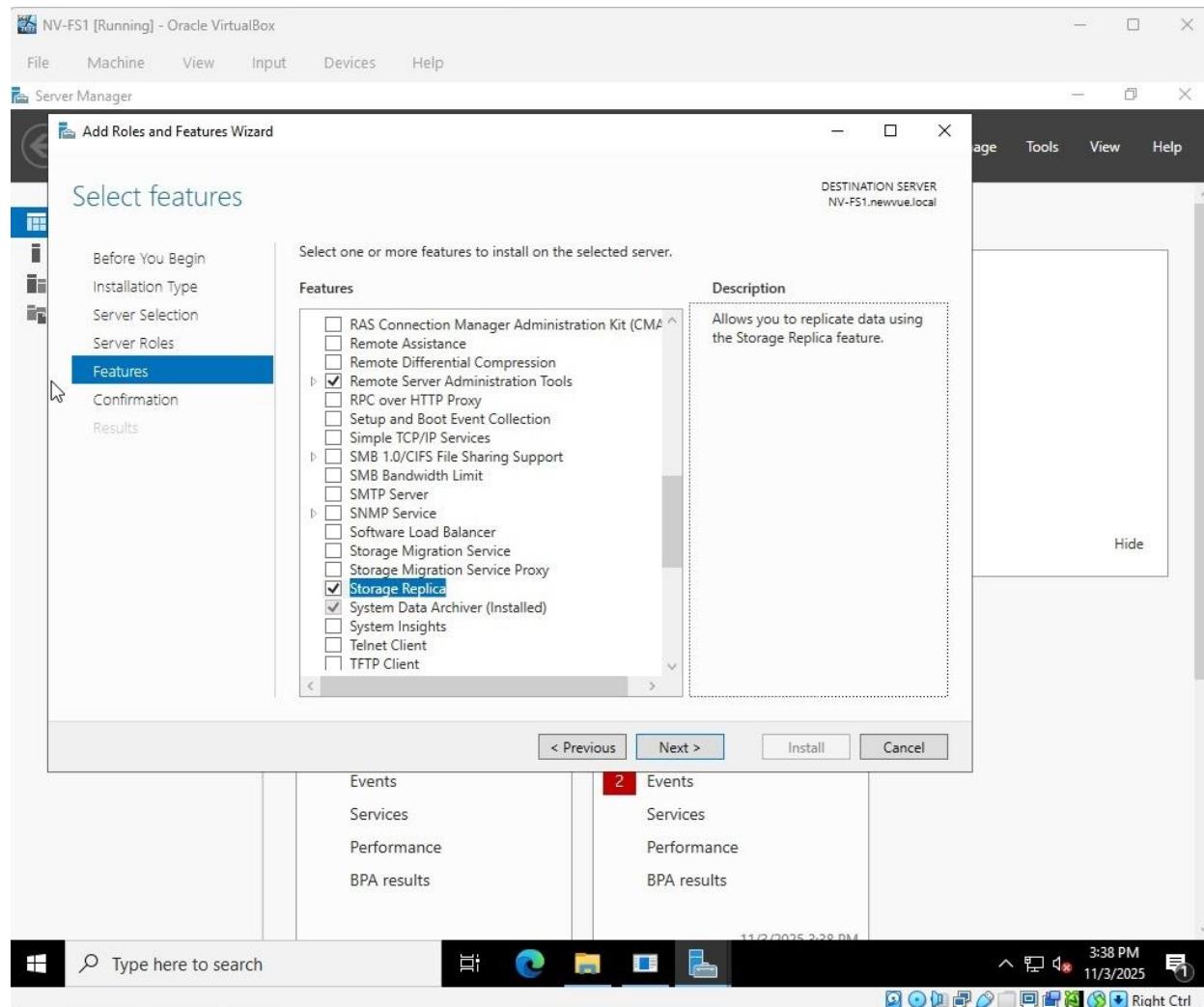
This section documents the technical steps carried out during the implementation of **Storage Replica** and the corresponding evidence that validates successful configuration. Each subsection outlines the task objectives, describes the specific focus of the implementation, and identifies the required screenshots or command outputs that confirm correct execution and functionality.

Task 1 – Install and Verify the Storage Replica Feature (20 pts)

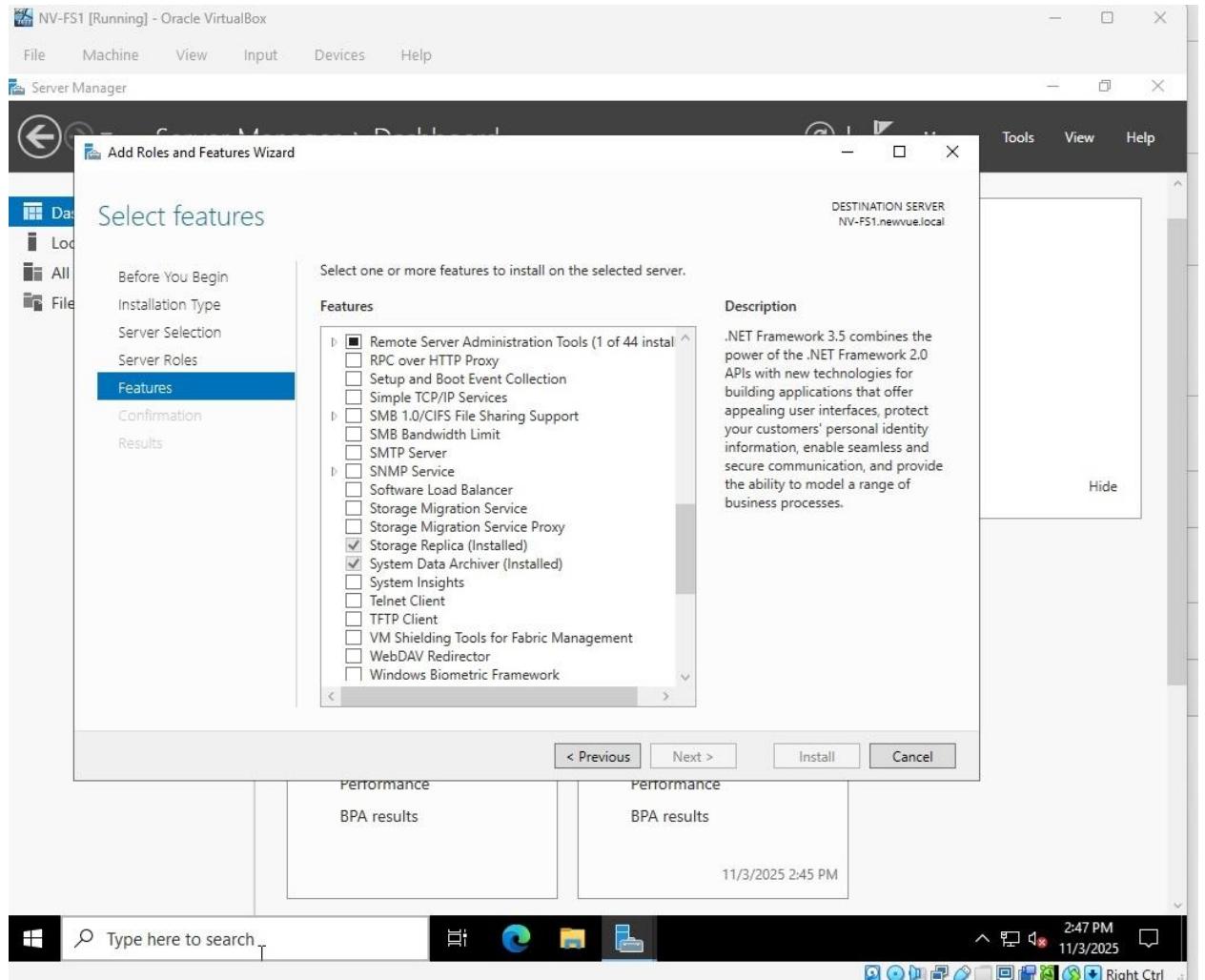
This task involved enabling the Storage Replica feature on both NV-FS1 and NV-DC1 to allow block-level replication and high-availability services. The installation was completed through Server Manager on both systems.

Evidence Requirements:

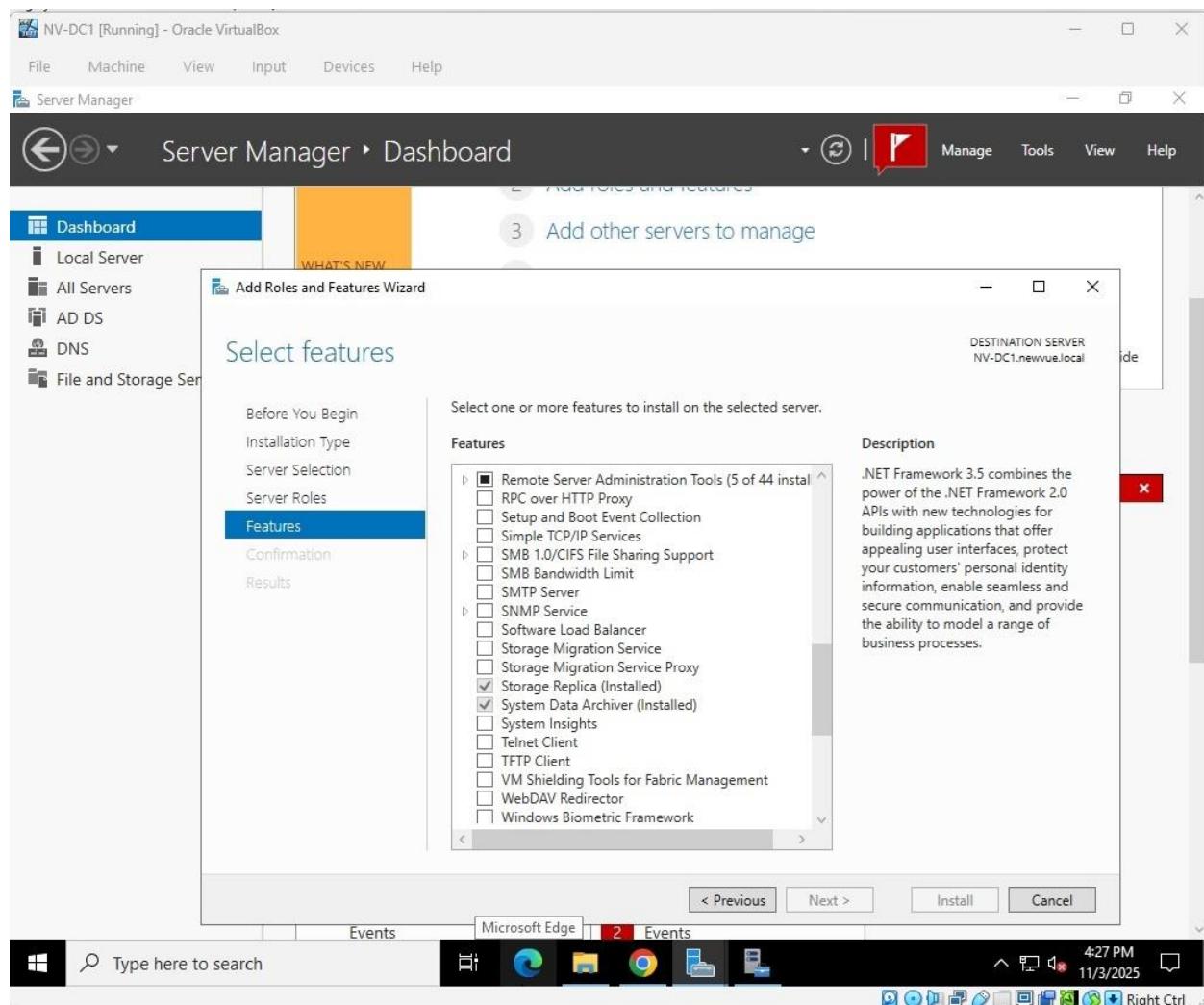
- Evidence 1:** Storage Replica selected in Add Roles and Features wizard (NV-FS1).



- **Evidence 2:** Installation summary showing completion on NV-FS1.



- **Evidence 3:** Storage Replica listed under Installed Features on NV-DC1.

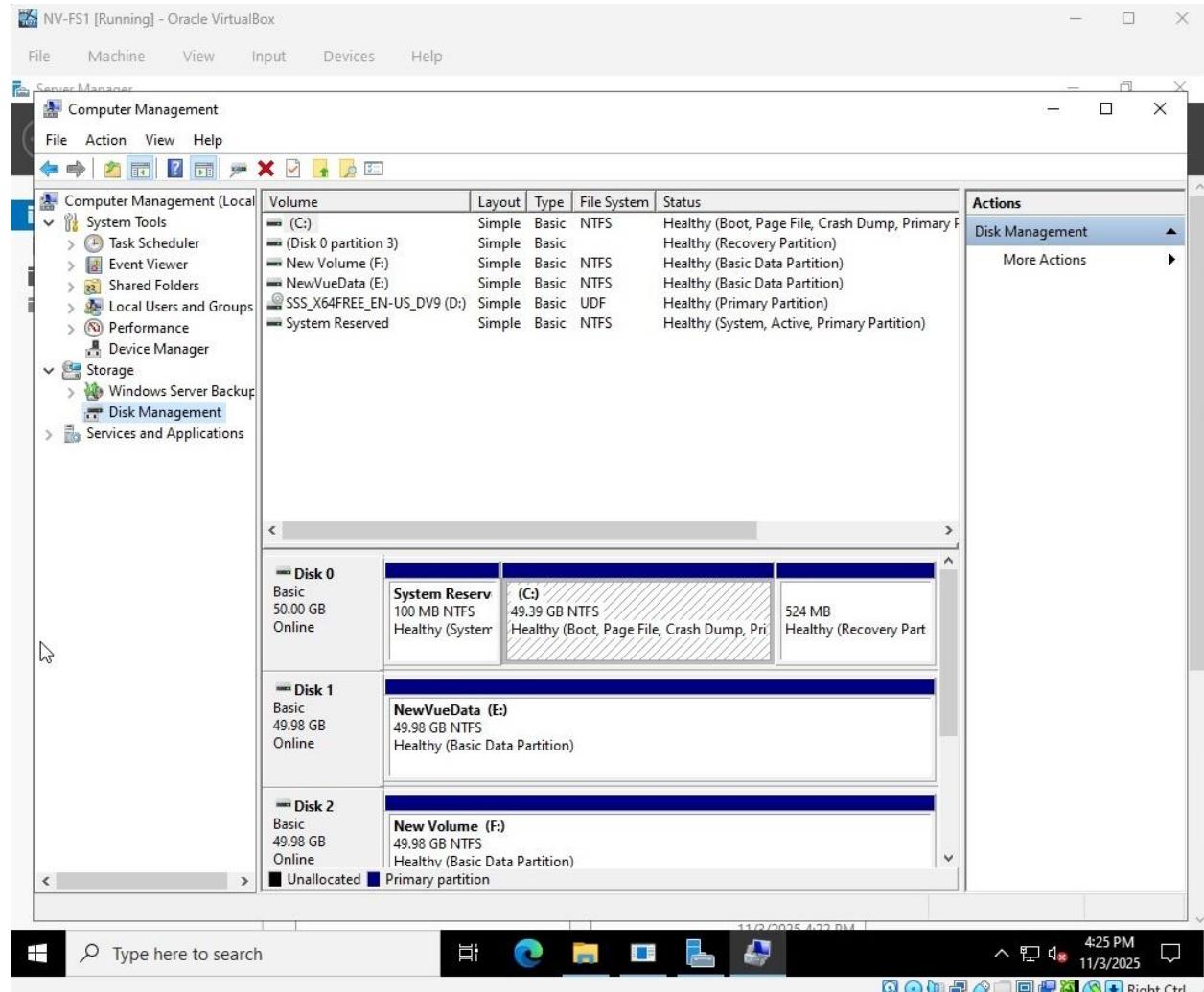


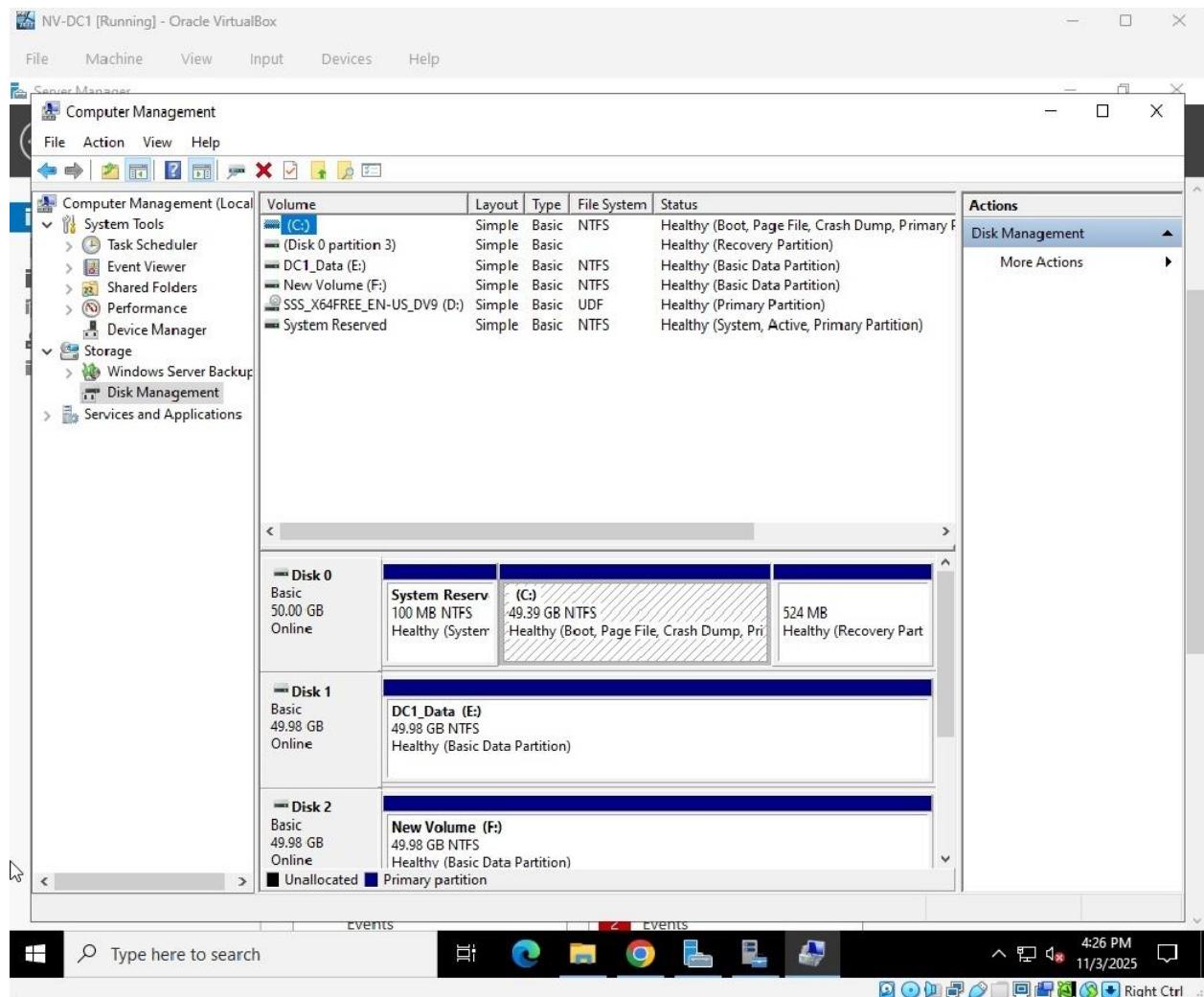
Task 2 – Prepare Volumes for Replication (10 pts)

In this section, additional virtual disks were attached and configured to serve as data and log volumes on both servers. Proper volume preparation is critical for efficient replication and log management.

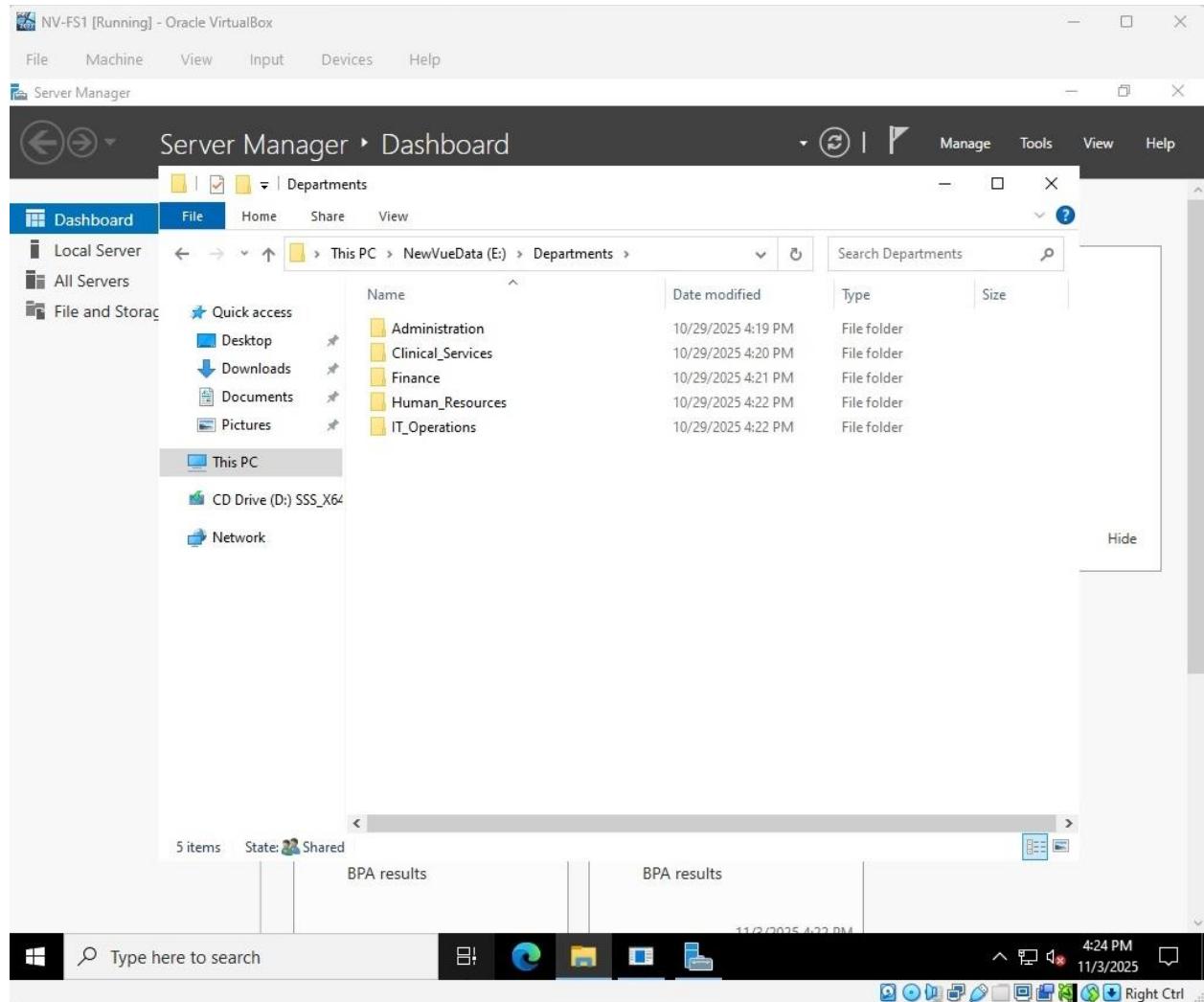
Evidence Requirements:

- **Evidence 4:** Disk Management showing data and log volumes on both servers.





- **Evidence 5:** Screenshot of E:\Departments on NV-FS1 displaying departmental folders.

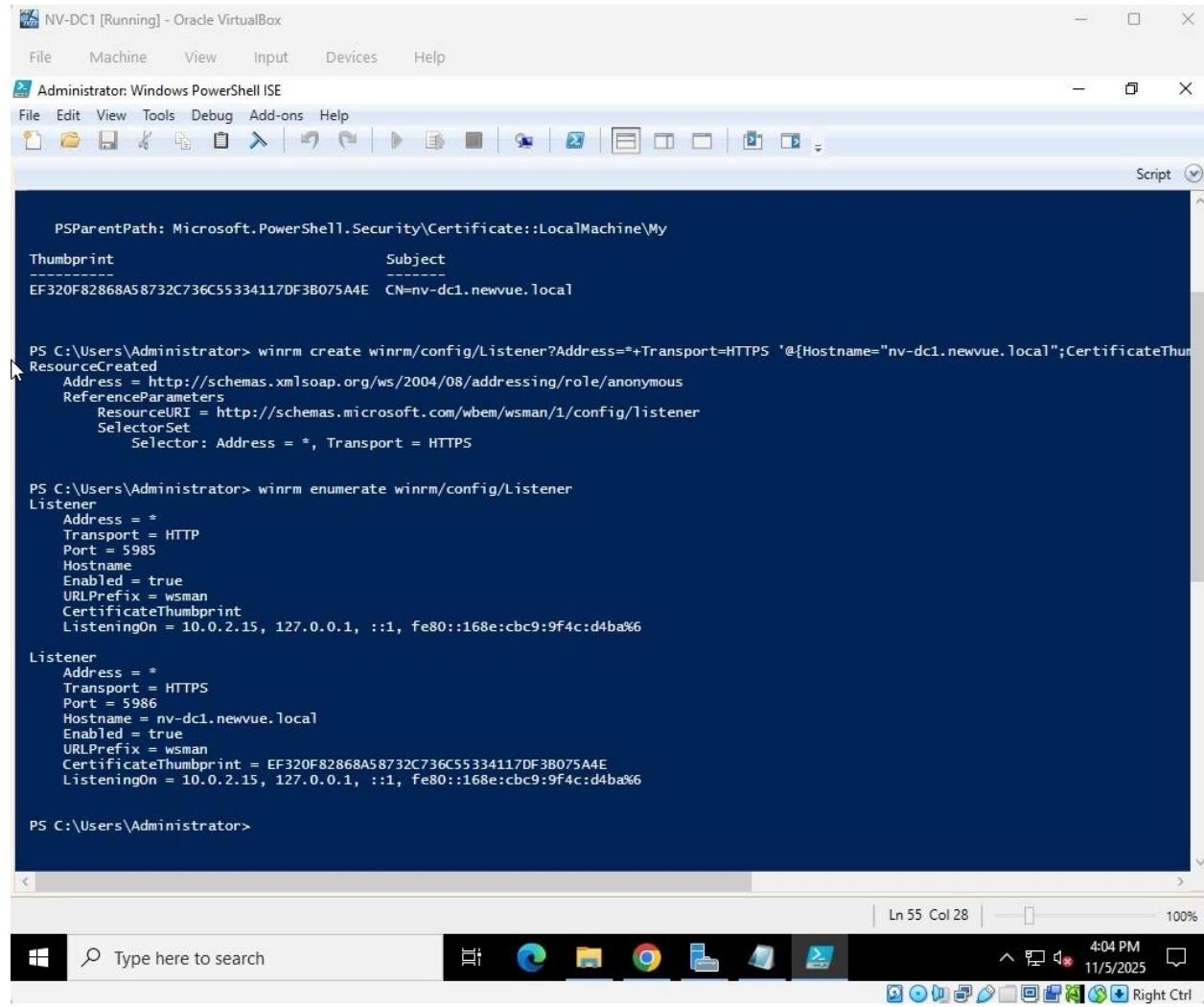


Task 3 – Configure WinRM over HTTPS and Establish Mutual Certificate Trust (20 pts)

This task focused on securing inter-server communication through encrypted HTTPS management sessions. Self-signed certificates were created and exchanged between NV-FS1 and NV-DC1 to establish mutual authentication and secure PowerShell remoting.

Evidence Requirements:

- Evidence 6a:** WinRM HTTPS listener configuration on NV-DC1.



The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE". The window displays PowerShell commands and their output related to configuring a WinRM HTTPS listener on NV-DC1.

```
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint          Subject
-----          -----
EF320F82868A58732C736C55334117DF3B075A4E CN=nv-dc1.newvue.local

PS C:\Users\Administrator> winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="nv-dc1.newvue.local";CertificateThumbprint=EF320F82868A58732C736C55334117DF3B075A4E}
ResourceCreated
  Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
  ReferenceParameters
    ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
  SelectorSet
    Selector: Address = *, Transport = HTTPS

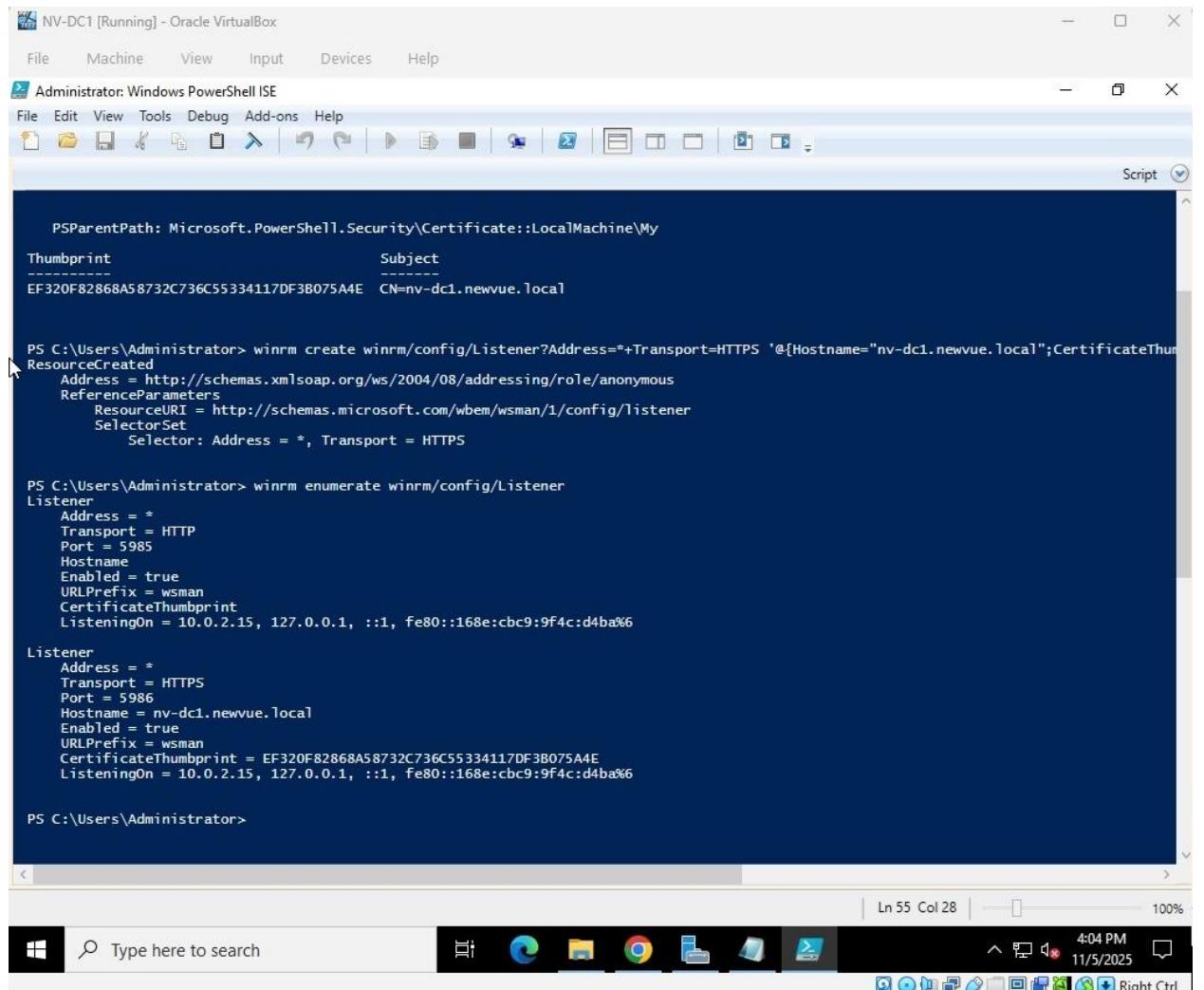
PS C:\Users\Administrator> winrm enumerate winrm/config/Listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 10.0.2.15, 127.0.0.1, ::1, fe80::168e:cbc9:9f4c:d4ba%6

Listener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname = nv-dc1.newvue.local
  Enabled = true
  URLprefix = wsman
  CertificateThumbprint = EF320F82868A58732C736C55334117DF3B075A4E
  ListeningOn = 10.0.2.15, 127.0.0.1, ::1, fe80::168e:cbc9:9f4c:d4ba%6

PS C:\Users\Administrator>
```

The PowerShell session shows the creation of a new HTTPS listener on port 5986 using a self-signed certificate with thumbprint EF320F82868A58732C736C55334117DF3B075A4E. It also lists the existing listeners, which include an HTTP listener on port 5985 and the newly created HTTPS listener on port 5986.

- **Evidence 6b:** WinRM HTTPS listener configuration on NV-FS1.



```

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint                               Subject
-----                                     -----
EF320F82868A58732C736C55334117DF3B075A4E CN=nv-dc1.newvue.local

PS C:\Users\Administrator> winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="nv-dc1.newvue.local";CertificateThumbprint=EF320F82868A58732C736C55334117DF3B075A4E}
ResourceCreated
  Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
  ReferenceParameters
    ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
    SelectorSet
      Selector: Address = *, Transport = HTTPS

PS C:\Users\Administrator> winrm enumerate winrm/config/Listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
    ListeningOn = 10.0.2.15, 127.0.0.1, ::1, fe80::168e:cbc9:9f4c:d4ba%6

Listener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname = nv-dc1.newvue.local
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = EF320F82868A58732C736C55334117DF3B075A4E
  ListeningOn = 10.0.2.15, 127.0.0.1, ::1, fe80::168e:cbc9:9f4c:d4ba%6

PS C:\Users\Administrator>

```

The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE" running on a virtual machine named "NV-DC1 [Running] - Oracle VirtualBox". The window displays PowerShell commands for managing WinRM listeners. The first command creates a new HTTPS listener with the specified host name and certificate thumbprint. The second command lists all existing WinRM listeners, showing two entries: one for HTTP on port 5985 and one for HTTPS on port 5986, both configured to listen on all interfaces (indicated by the asterisk) and using the wsman URL prefix. The PowerShell session ends with a final command prompt.

- **Evidence 6c:** Certificates imported into Trusted Root Certification Authorities on both servers.

NV-DC1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

Certificates (Local Computer) Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authority Trusted Publishers Untrusted Certificates Third-Party Root Certification Trusted People Client Authentication Issuer Preview Build Roots Test Roots Certificate Enrollment Request Smart Card Trusted Roots Trusted Packaged App Installation Trusted Devices Windows Live ID Token Issue WindowsServerUpdateService

Issued To	Issued By	Expiration Date	Intended Purposes	Actions
Class 3 Public Primary Certificate...	Class 3 Public Primary Certificatio...	8/1/2028	Client Authenticati...	Certificates More Actions
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Mic
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...	Dig
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	Dig
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	Dig
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati...	Dig
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	Glo
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Mic
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Mic
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Mic
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Mic
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/22/2039	<All>	Mic
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time Stamping	Veri
nv-fs1.newvve.local	nv-fs1.newvve.local	11/5/2026	Client Authenticati...	<N
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032	Code Signing	<N
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Tha
WindowsAdminCenterSelfSigned	WindowsAdminCenterSelfSigned	1/2/2026	Server Authenticati...	<N

Type here to search 4:18 PM 11/5/2025 Right Ctrl

NV-FS1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

Actions

Certificates

More Actions ▾

Issued To	Issued By	Expiration Date	Intend
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Client
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time S
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/22/2039	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time S
nv-dc1.newvue.local	nv-dc1.newvue.local	11/5/2026	Client
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032	Code S
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time S
WindowsAdminCenterSelfSigned	WindowsAdminCenterSelfSigned	1/2/2026	Server

Type here to search

4:36 PM
11/5/2025

Right Ctrl

- **Evidence 6d:** Successful Test-WSMan -UseSSL results confirming secure connectivity.

```

NV-DC1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

PrimaryStatus      : OK
Status            : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource  : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId       :

PS C:\Users\Administrator> Test-NetConnection nv-fs1.newvue.local -Port 5986

ComputerName      : nv-fs1.newvue.local
RemoteAddress     : 10.0.2.17
RemotePort        : 5986
InterfaceAlias    : Ethernet
SourceAddress     : 10.0.2.15
TcpTestSucceeded : True

PS C:\Users\Administrator> Test-WSMan nv-fs1.newvue.local -UseSSL

wsmid           : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor   : Microsoft Corporation
ProductVersion  : OS: 0.0.0 SP: 0.0 Stack: 3.0

PS C:\Users\Administrator>

```

The screenshot shows a Windows PowerShell ISE window titled "NV-DC1 [Running] - Oracle VirtualBox". The window contains several PowerShell commands and their outputs. The commands include "Test-NetConnection" and "Test-WSMan" with the "-UseSSL" parameter. The outputs provide details about network connections and WSMAN identity, such as computer names, remote addresses, ports, and protocol versions. The PowerShell window has a standard Windows interface with a menu bar, toolbar, and status bar at the bottom.

NV-FS1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded : False

```
PS C:\Users\Administrator.NEWVUE> ping 10.0.2.15
Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PS C:\Users\Administrator.NEWVUE> Test-NetConnection nv-dc1.newvue.local -Port 5986

ComputerName      : nv-dc1.newvue.local
RemoteAddress     : 10.0.2.15
RemotePort         : 5986
InterfaceAlias    : Ethernet
SourceAddress     : 10.0.2.17
TcpTestSucceeded  : True
```

```
PS C:\Users\Administrator.NEWVUE> Test-WSMan nv-dc1.newvue.local -UseSSL

wsmanid          : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion   : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor     : Microsoft Corporation
ProductVersion    : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

```
PS C:\Users\Administrator.NEWVUE>
```

Completed

Type here to search

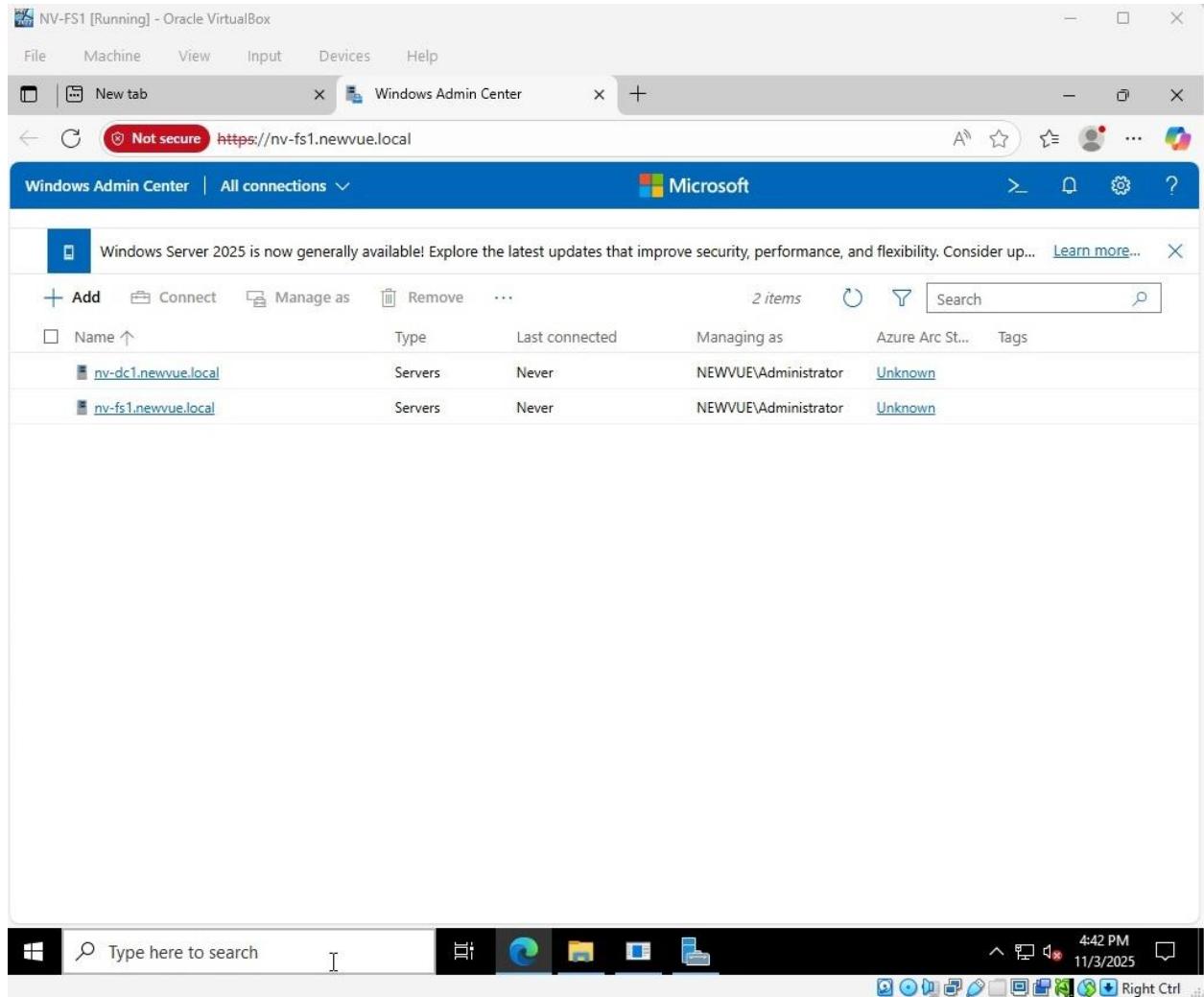
Ln 123 Col 35 4:46 PM 11/5/2025 Right Ctrl

Task 4 – Install and Configure Windows Admin Center (10 pts)

Windows Admin Center was installed on NV-FS1 to centrally manage servers and monitor replication status. Both NV-FS1 and NV-DC1 were added for management and verification.

Evidence Requirements:

- **Evidence 7:** Screenshot showing successful WAC login on NV-FS1.

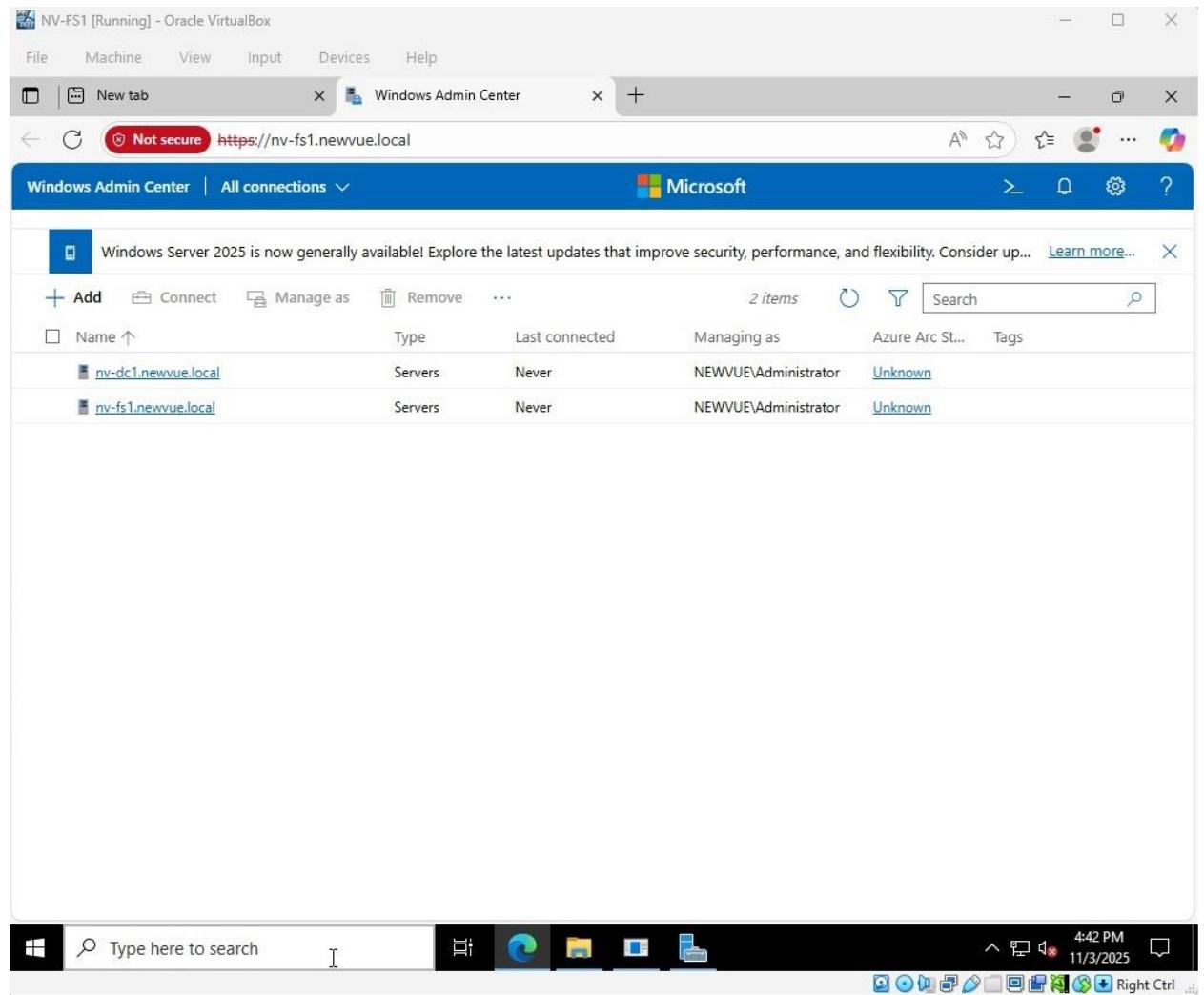


The screenshot shows the Windows Admin Center interface running in a browser window titled "NV-FS1 [Running] - Oracle VirtualBox". The URL is https://nv-fs1.newvue.local. The main content area displays a table of connected servers:

Name	Type	Last connected	Managing as	Azure Arc St...	Tags
nv-dc1.newvue.local	Servers	Never	NEWVUE\Administrator	Unknown	
nv-fs1.newvue.local	Servers	Never	NEWVUE\Administrator	Unknown	

The taskbar at the bottom shows the Windows Start button, a search bar, and several pinned icons. The system tray indicates the date and time as 11/3/2025 at 4:42 PM.

- **Evidence 8:** Screenshot showing both servers connected in WAC under All Connections.



The screenshot shows the Windows Admin Center interface running in a browser window titled "NV-FS1 [Running] - Oracle VirtualBox". The URL is <https://nv-fs1.newvue.local>. The main content area displays a table of connected servers:

Name	Type	Last connected	Managing as	Azure Arc St...	Tags
nv-dc1.newvue.local	Servers	Never	NEWVUE\Administrator	Unknown	
nv-fs1.newvue.local	Servers	Never	NEWVUE\Administrator	Unknown	

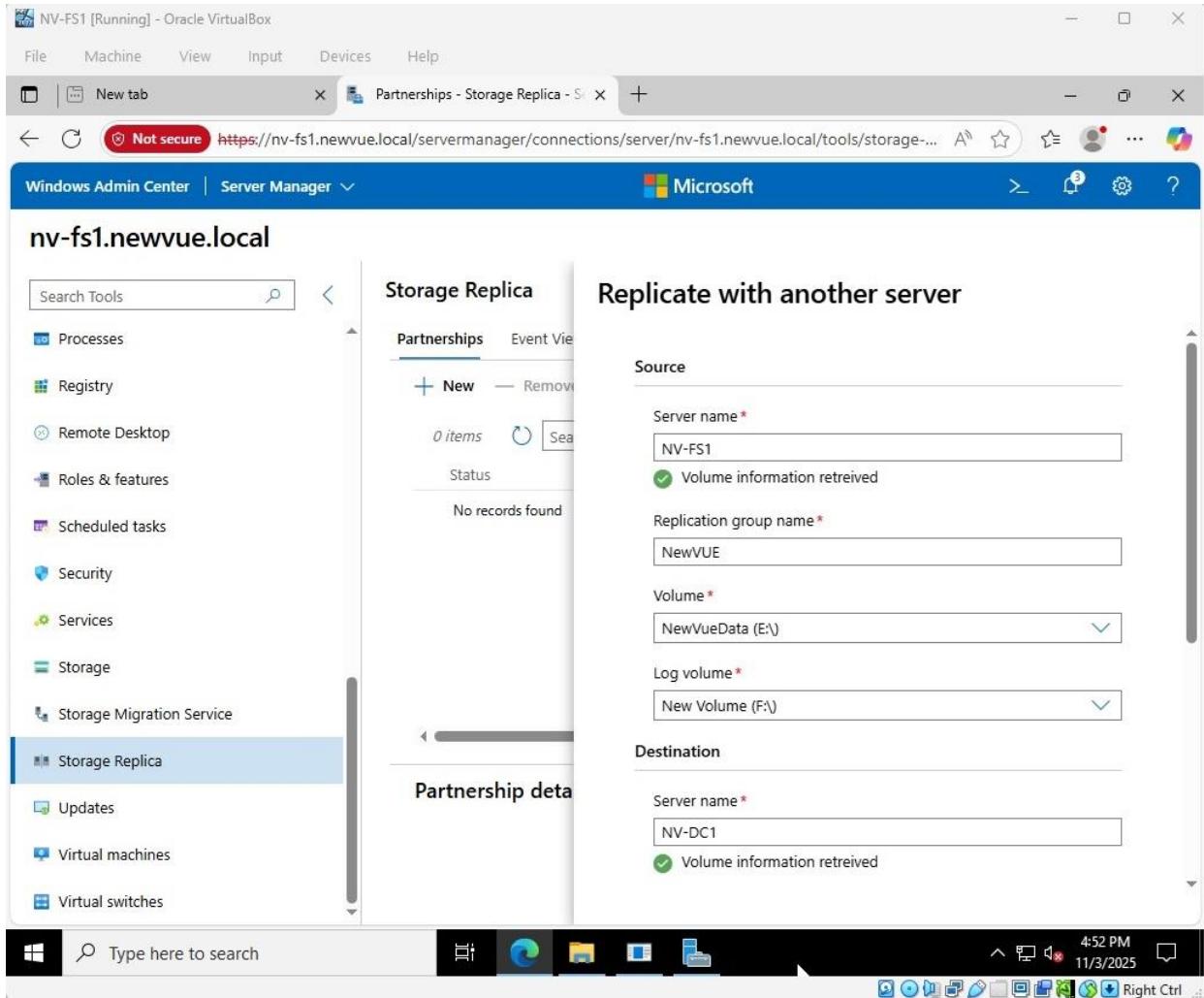
The Windows taskbar at the bottom shows the search bar, pinned icons for File Explorer, Edge, and File History, and the system tray with the date and time (4:42 PM, 11/3/2025).

Task 5 – Create and Configure Replication Partnership (30 pts)

A replication partnership was established between NV-FS1 and NV-DC1 using Windows Admin Center. Synchronous replication mode was selected to ensure zero data loss between both servers.

Evidence Requirements:

- Evidence 9:** Screenshot showing replication configuration summary in WAC.



NV-FS1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

New tab Partnerships - Storage Replica - S

Not secure https://nv-fs1.newvue.local/servermanager/connections/server/nv-fs1.newvue.local/tools/storage-... A ⚡ ⚡ ...

Windows Admin Center | Server Manager Microsoft

nv-fs1.newvue.local

Search Tools

Processes Registry Remote Desktop Roles & features Scheduled tasks Security Services Storage Storage Migration Service Storage Replica Updates Virtual machines Virtual switches

Partnerships Event View

+ New Remove

0 items Status No records found

Storage Replica

Partnership data

Replicate with another server

Server name * NV-DC1 Volume information retrieved

Replication group name * NewVUE

Volume * DC1_Data (E:\)

Log volume * New Volume (F:\)

More options

Log size, asynchronous replication, encryption, seeding with source files, consistency groups

Create Cancel

Type here to search

4:53 PM 11/3/2025 Right Ctrl

- **Evidence 10:** Screenshot confirming successful partnership creation and synchronization.

The screenshot shows the Windows Admin Center interface for the server **nv-fs1.newvue.local**. The left sidebar navigation bar is visible, with the **Storage Replica** item selected. The main content area displays the **Storage Replica** section under the **Partnerships** tab. A table lists one item, showing the status as **Continuously replicating**, the source node as **NV-FS1**, the source group name as **NewVUE**, and the source data volume as **E:**.

Status	Source node	Source group name	Source data volume
✓ Continuously replicating	NV-FS1	NewVUE	E:\

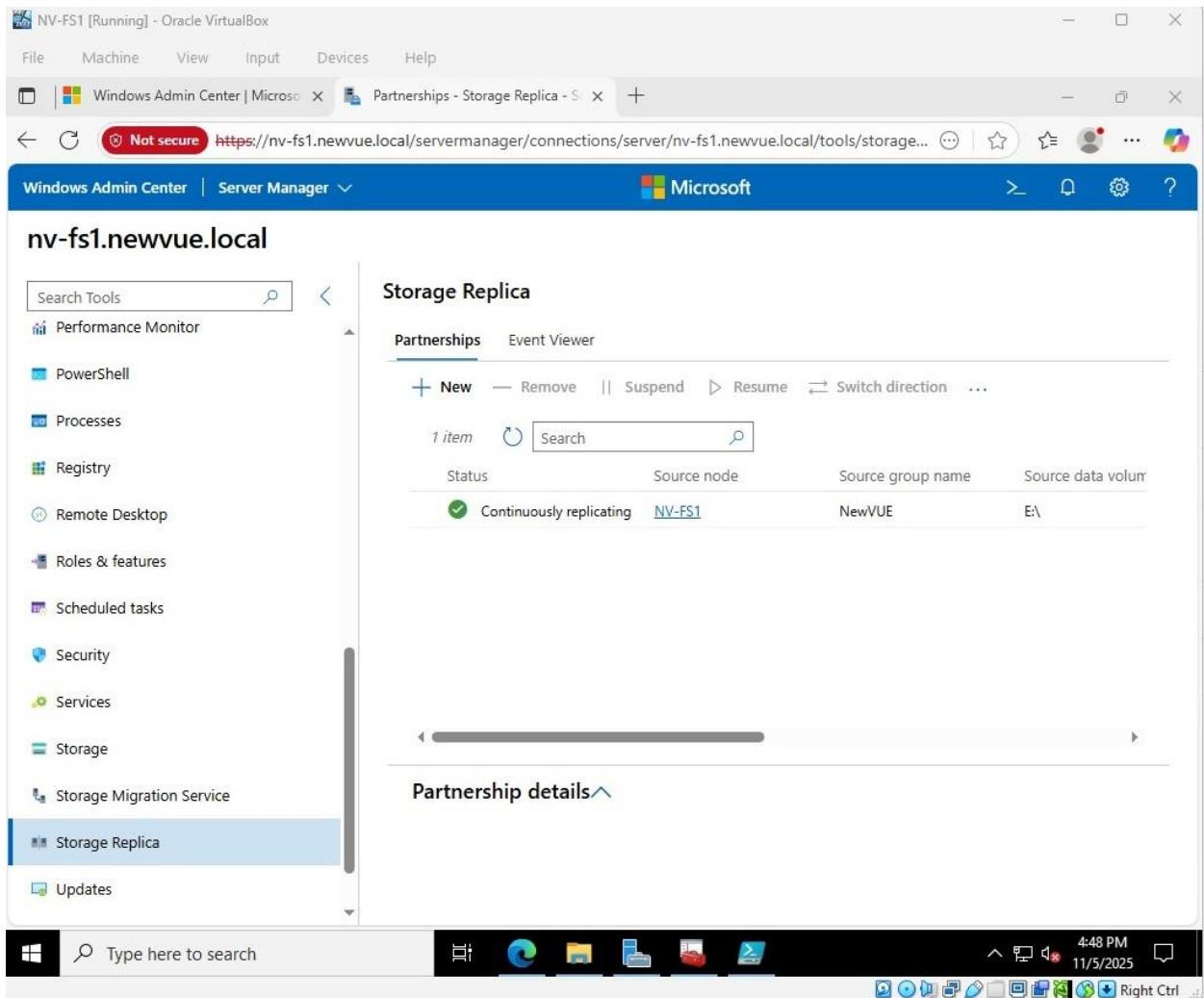
At the bottom of the screen, the taskbar shows the date and time as **11/5/2025 4:48 PM**.

Task 6 – Monitor, Validate, and Simulate Failure (40 pts)

This task verified replication health, validated synchronization status, and simulated a failure scenario to confirm read-only access to replicated data. Replication status and direction were confirmed in both Windows Admin Center and PowerShell using the Get-SRGroup and Get-SRPartnership cmdlets.

Evidence Requirements:

- **Evidence 11:** Screenshot showing replication status = *Continuously Replicating*.

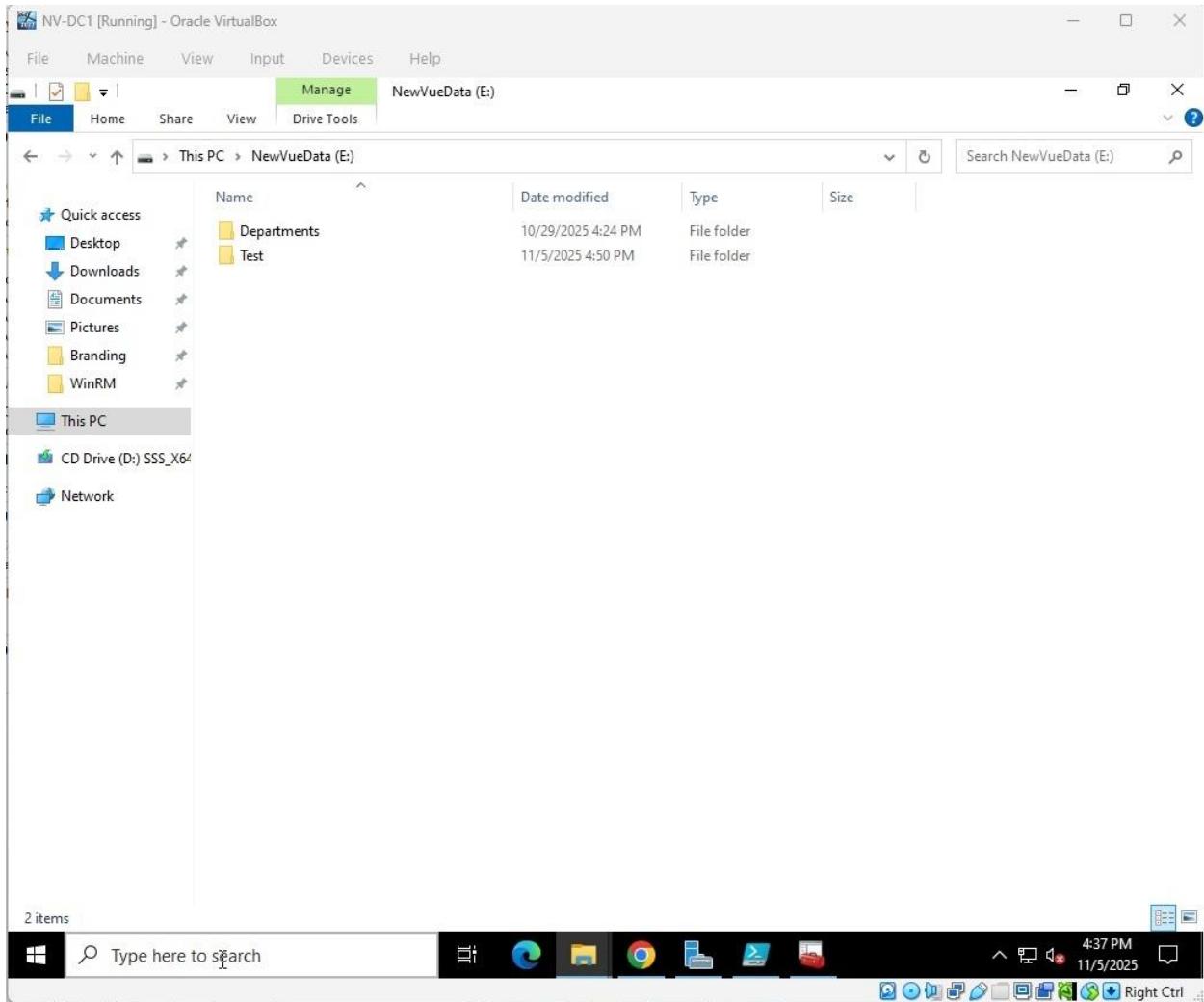


- **Evidence 12a:** Screenshot of **Partnerships** view showing replication health.

The screenshot shows the Windows Admin Center interface for the server **nv-fs1.newvue.local**. The left sidebar lists various management tools, and the main content area displays the **Partnerships - Storage Replica** view. A table compares the replication configuration for a specific log volume between the **Source** (Computer name: NV-FS1) and the **Destination** (Computer name: NV-DC1).

Replication group		Replicated volume	
Source	Destination	Source	Destination
Name NewVUE	Computer name NV-FS1	Name NewVUE	Computer name NV-DC1
Log volume F:\	Log size 8 GB	Log volume F:\	Log size 8 GB
Write Consistency Disabled	Recovery point objective None	Write Consistency Disabled	Recovery point objective None
Encryption Disabled	Number of replicas 1	Encryption Disabled	Number of replicas 1
Replication mode Synchronous	Replication status Continuously replicating	Replication mode Synchronous	Replication status Continuously replicating
Log type Traditional		Log type Traditional	

- **Evidence 12b:** Screenshot of E:\Departments on NV-DC1 after **Switch Direction** showing Replication_Test.



- **Evidence 12c:** Screenshot of PowerShell output from Get-SRGroup and Get-SRPartnership.

```

NV-FS1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

PS C:\Users\Administrator.NEWVUE> Get-SRGroup

AllowVolumeResize : False
AsyncRPO          :
ComputerName      : NV-FS1
Description       :
Id               : 2586ca64-0916-4795-8b67-2988521f008e
IsAutoFailover   :
IsCluster         :
IsCompressed     :
IsEncrypted       :
IsInPartnership  :
IsMounted         :
IsPrimary         :
IsSuspended       :
IsWriteConsistency :
LastInSyncTime   :
LogSizeInBytes   : 8589934592
LogType           : FileBased
LogVolume         : F:\\
Name              : NewVUE
NumOfReplicas    : 1
Partitions        : {7a093e7a-6539-4c3b-abd3-b030b1f63d85}
Replicas          : {MSFT_WvrReplica (PartitionId = "7a093e7a-6539-4c3b-abd3-b030b1f63d85")}
ReplicationMode   : Synchronous
ReplicationStatus : ContinuouslyReplicating
TemporaryPath    :
PSCoordinateName  :

PS C:\Users\Administrator.NEWVUE> Get-SRPartnership

DestinationComputerName : NV-DC1
DestinationRGName       : NewVUE
Id                      : c0657ba6-08cf-44fa-906f-32e65cef6903
SourceComputerName      : NV-FS1
SourceRGName            : NewVUE
PSCoordinateName        :

Completed
Ln 69 Col 35 | 100%
4:41 PM 11/5/2025
Type here to search
Right Ctrl

```

Below evidence were unable to obtain due to error encountered and time.

- **Evidence 13a:** Screenshot showing E: online on NV-DC1 during NV-FS1 outage.
- **Evidence 13b:** Screenshot showing Access Denied when modifying data.
- **Evidence 13c:** Screenshot of PowerShell output showing replication paused/resumed.
- **Evidence 13d:** Screenshot showing replication resumed after recovery.

Section 3: Summary of Results (10 pts)

The implementation of Storage Replica was successfully completed, establishing a robust core replication partnership between NV-FS1 and NV-DC1. Key achievements include the successful installation of the Storage Replica feature, the secure configuration of WinRM over HTTPS for encrypted management communication, and the creation of a functional synchronous replication partnership via Windows Admin Center. Continuous monitoring confirmed a healthy replication status, with data synchronizing seamlessly from the source (NV-FS1) to the destination (NV-DC1) during normal operations.

A planned failure simulation was initiated to validate disaster recovery procedures. During this test, after simulating a failure of NV-FS1, the replicated data volume (E:) on NV-DC1 was confirmed to be "Online" in Disk Management, indicating the storage layer was active. However, an "NTFS" error prevented access to the volume via File Explorer, which halted further testing and prevented the collection of evidence (13a-d) to verify read-only client accessibility and detailed replication state changes.

This outcome confirms that the underlying block-level replication was operational but highlights a potential configuration issue with the file system mount point or access permissions on the destination volume during a failover event. Therefore, while the implementation proves the replication technology is sound, full validation of the business continuity failover process requires further investigation and testing.