

Configure and Manage the Virtualised Enterprise Network

Victoria Price
2315903

Evidence submitted using screenshots below.

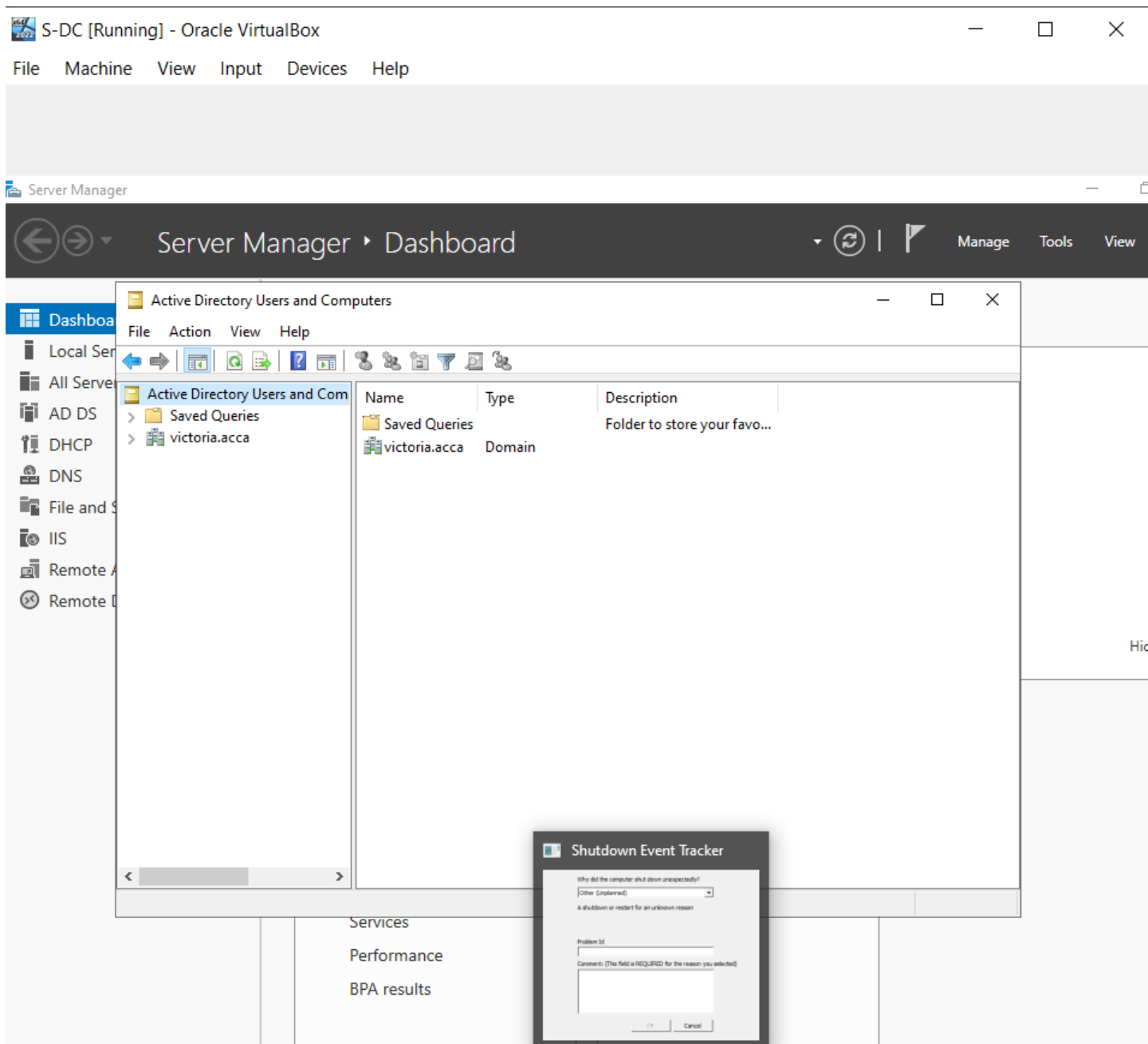


Figure 1: Active Directory Users and Computers - victoria.acca Domain Successfully Created

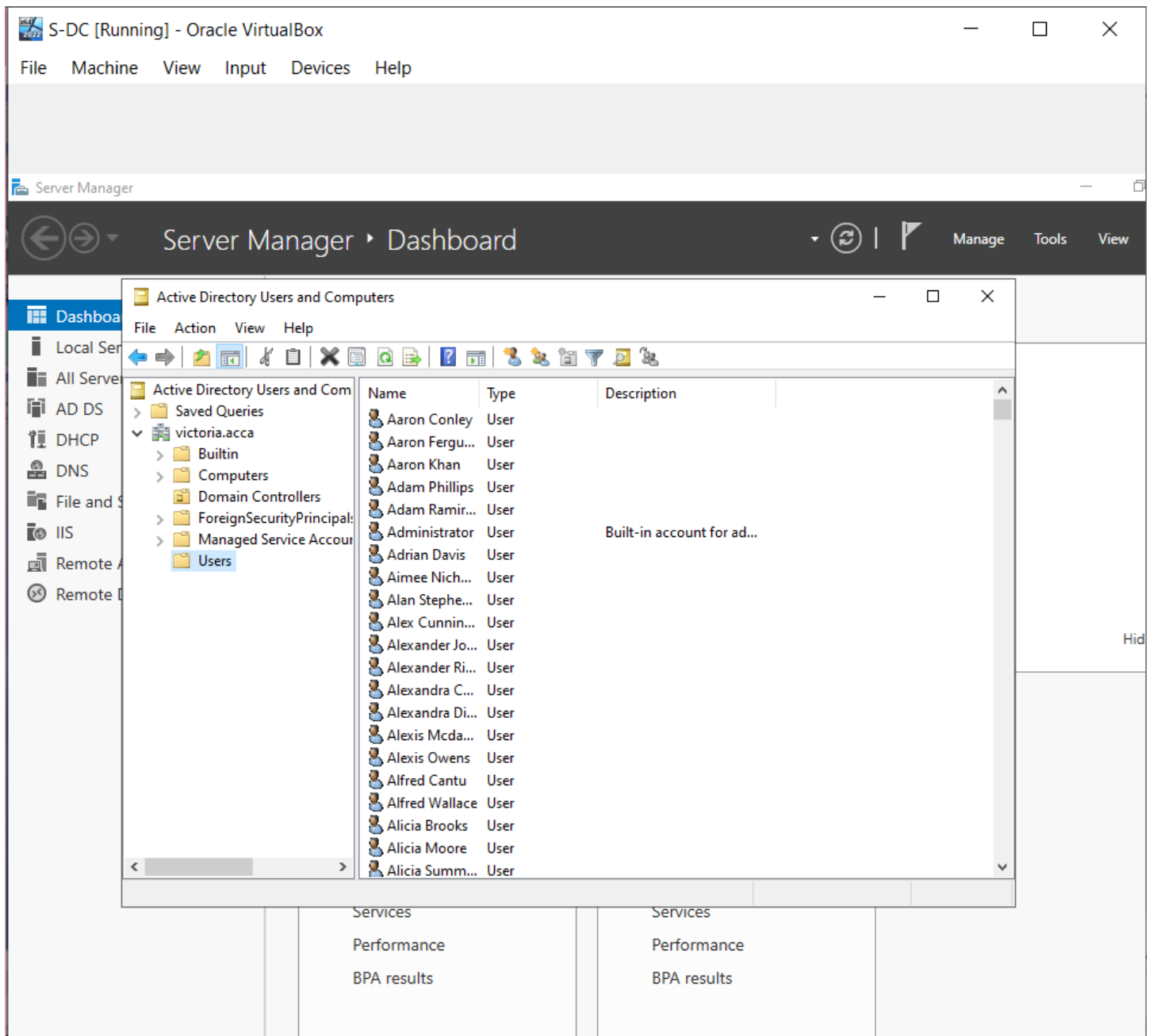


Figure 2: Active Directory Users and Computers - Bulk User Accounts Created via PowerShell Script

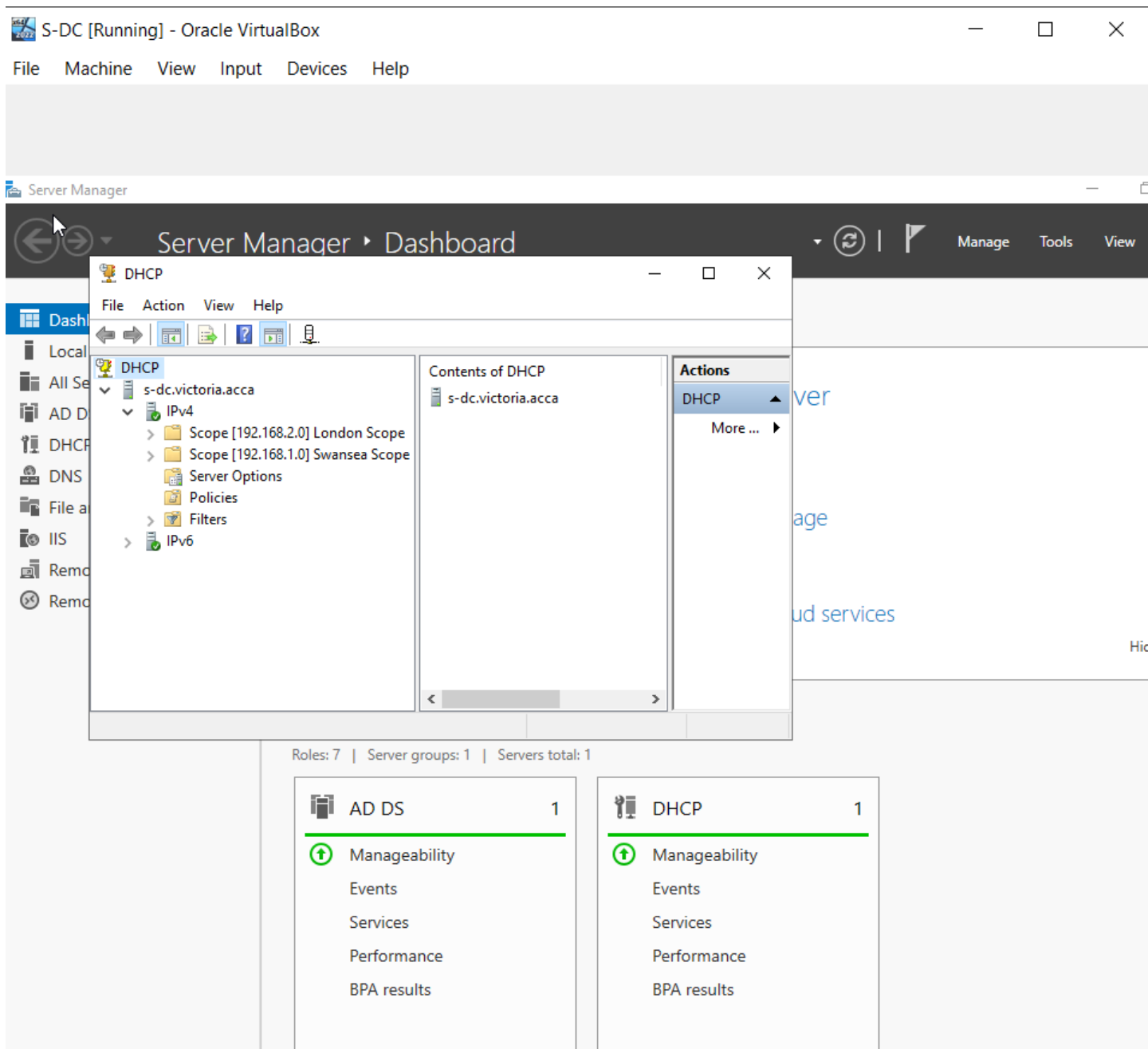
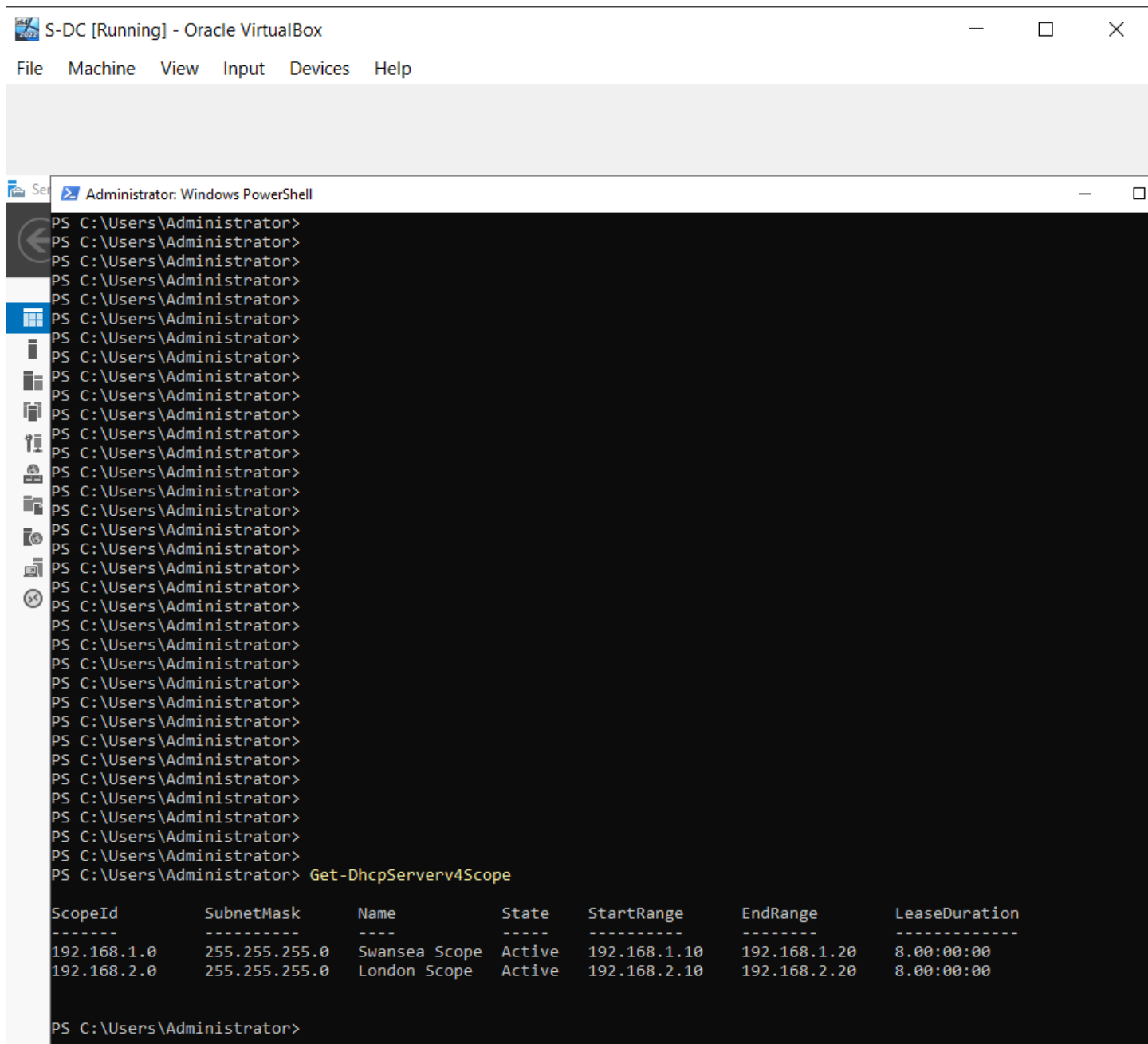


Figure 4: DHCP Manager - Swansea and London Scopes Configured on S-DC



The screenshot shows a Windows PowerShell console window titled "Administrator: Windows PowerShell". The prompt is "PS C:\Users\Administrator>". The command "Get-DhcpServerv4Scope" has been entered and executed. The output is a table with 7 columns: ScopeId, SubnetMask, Name, State, StartRange, EndRange, and LeaseDuration. The table contains two rows of data, both with a State of "Active".

ScopeId	SubnetMask	Name	State	StartRange	EndRange	LeaseDuration
192.168.1.0	255.255.255.0	Swansea Scope	Active	192.168.1.10	192.168.1.20	8.00:00:00
192.168.2.0	255.255.255.0	London Scope	Active	192.168.2.10	192.168.2.20	8.00:00:00

Figure 5: PowerShell Verification - Get-DhcpServerv4Scope Confirming Both Scopes Active

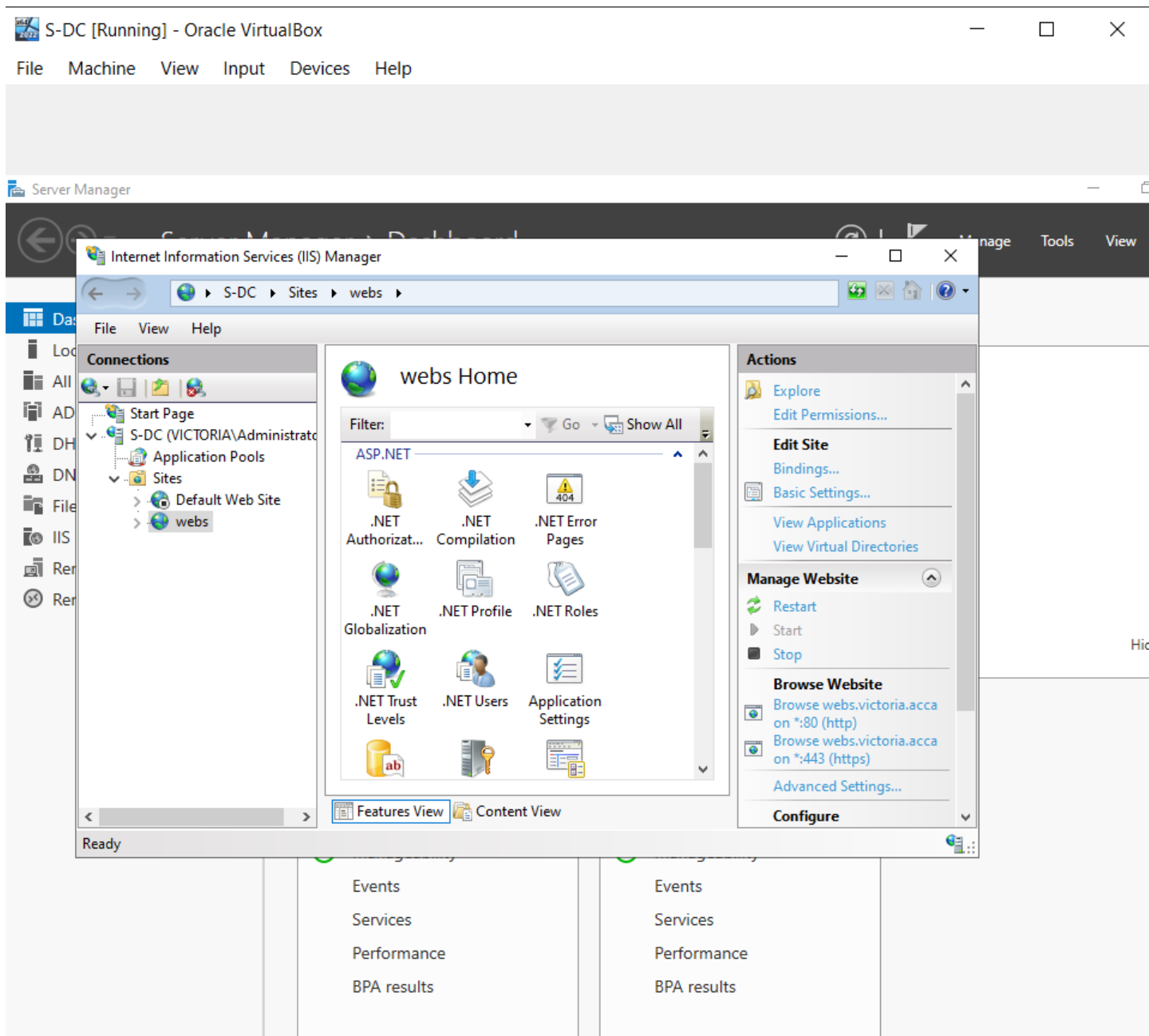


Figure 6: IIS Manager - 'webs' Site Running with HTTP and HTTPS Bindings on S-DC

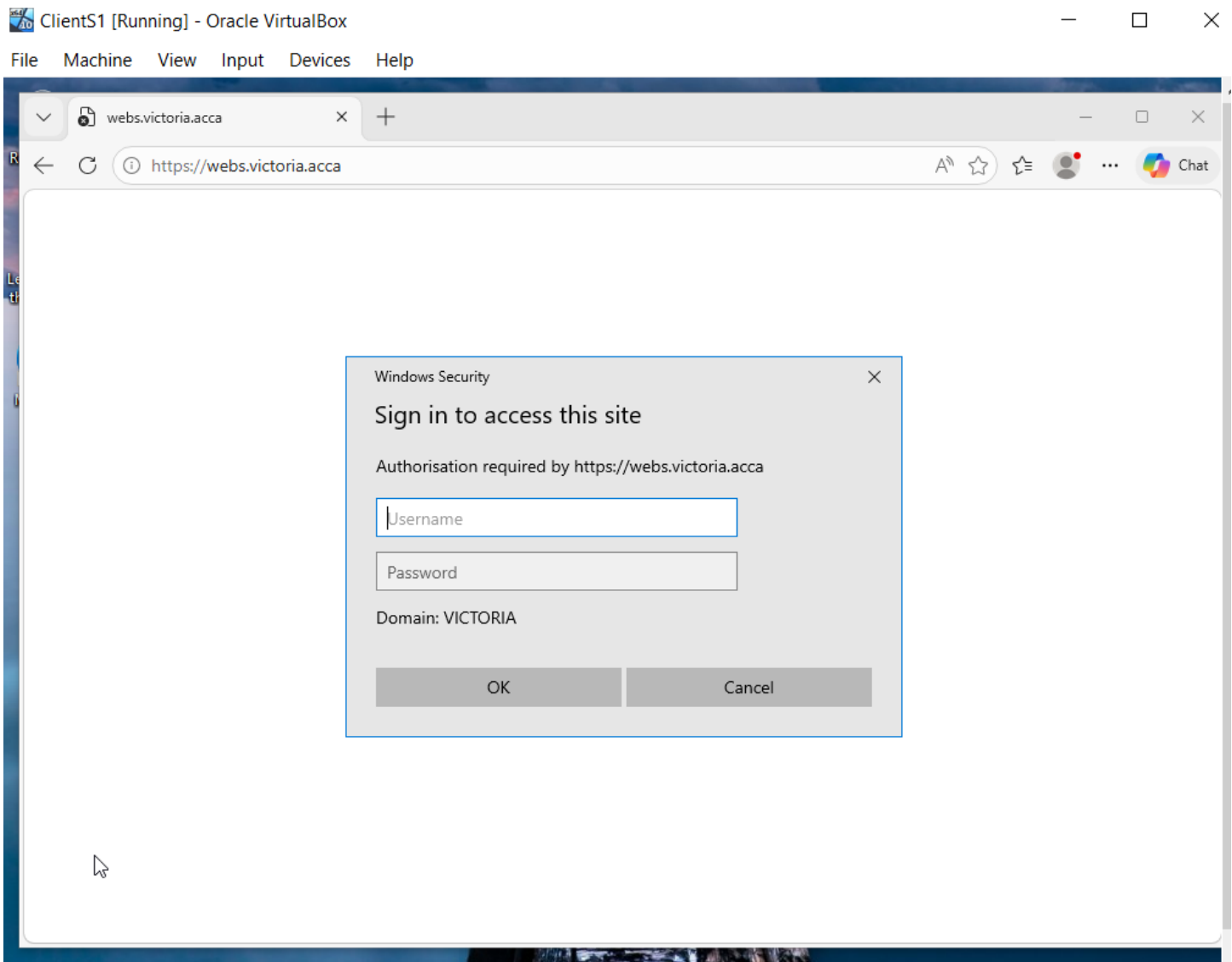


Figure 7: Windows Authentication Prompt - Accessing <https://webs.victoria.acca> from ClientS1

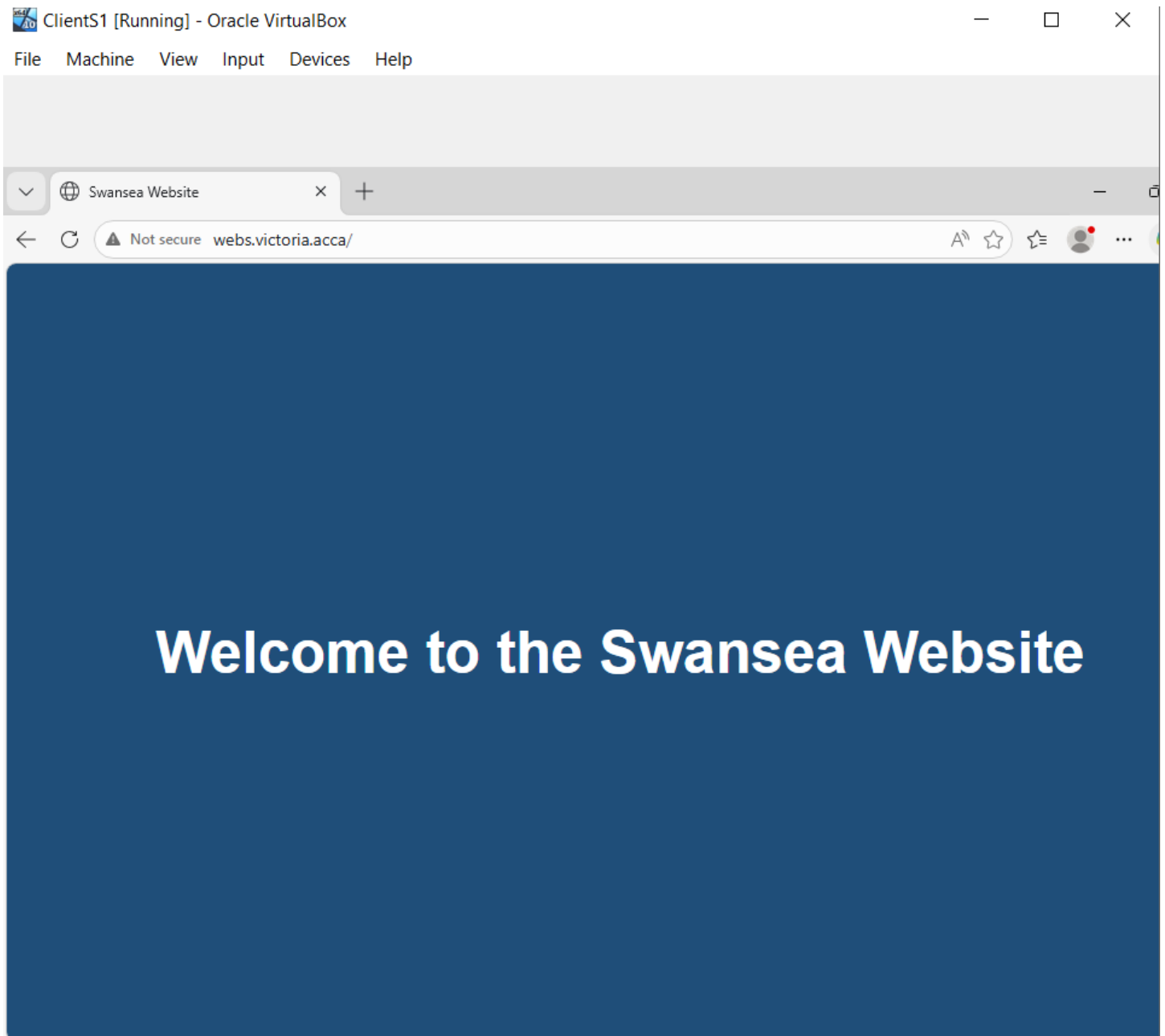


Figure 8: IIS Web Server - Welcome to the Swansea Website Successfully Displayed After Authentication

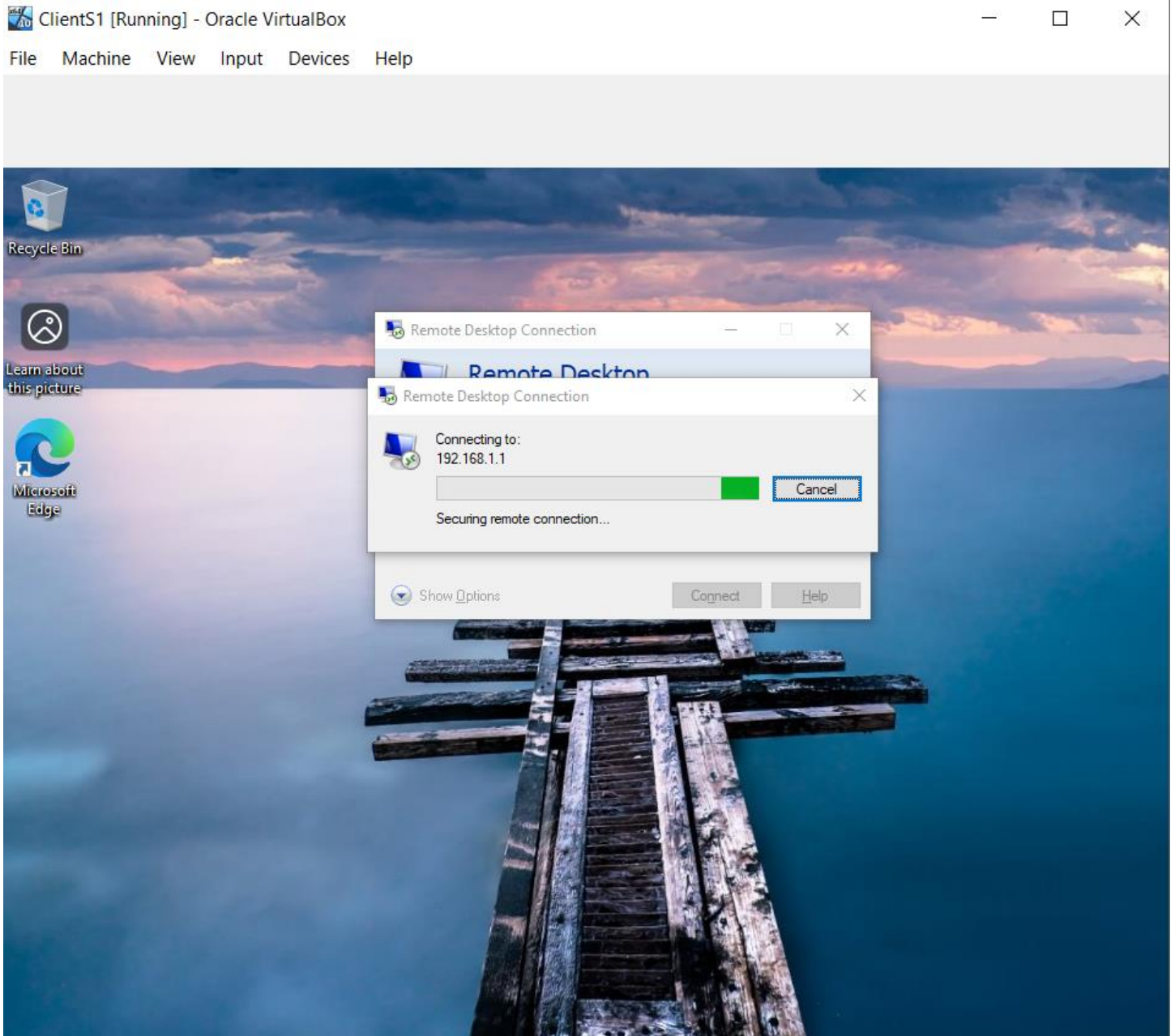


Figure 9: Remote Desktop Connection - ClientS1 Connecting to S-DC via 192.168.1.1

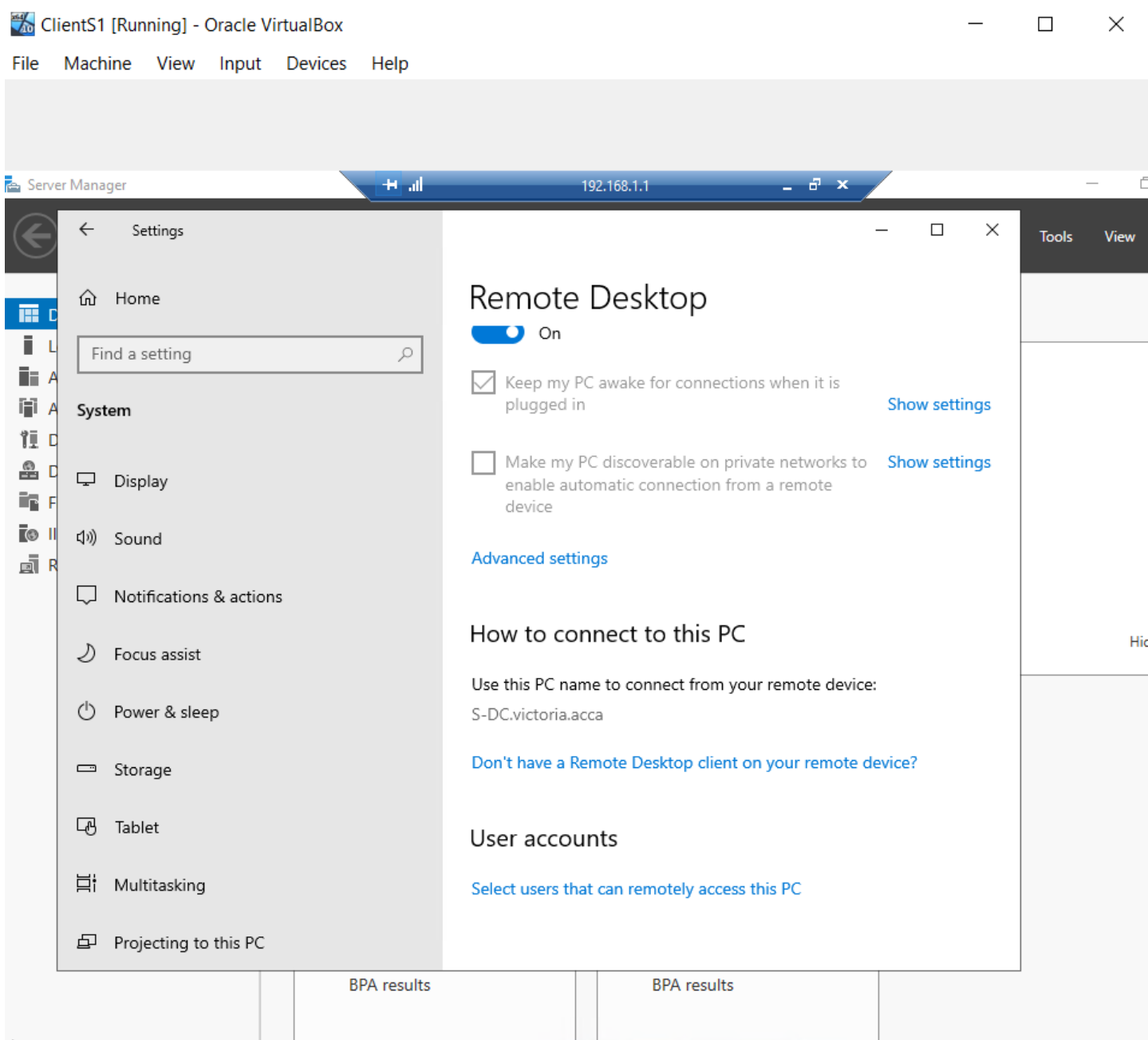


Figure 10: Remote Desktop Settings - RDP Enabled on S-DC.victoria.acca

S-DC [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Administrator: Windows PowerShell

DisplayName	Enabled	Direction	Action
Core Networking - Packet Too Big (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Parameter Problem (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Router Advertisement (ICMPv6-In)	True	Inbound	Allow
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	True	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv4-Out)	True	Outbound	Allow
Core Networking - Router Solicitation (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	True	Inbound	Allow
Core Networking - Multicast Listener Report v2 (ICMPv6-Out)	True	Outbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-Out)	False	Outbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-Out)	True	Outbound	Allow
Core Networking - Multicast Listener Done (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Router Solicitation (ICMPv6-In)	True	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv6-Out)	True	Outbound	Allow
Core Networking - Router Advertisement (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	True	Inbound	Allow
Core Networking - Parameter Problem (ICMPv6-In)	True	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	True	Inbound	Allow
Core Networking - Neighbor Discovery Advertisement (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Multicast Listener Query (ICMPv6-Out)	True	Outbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)	False	Inbound	Allow
Core Networking - Time Exceeded (ICMPv6-Out)	True	Outbound	Allow
Virtual Machine Monitoring (Echo Request - ICMPv4-In)	True	Inbound	Allow
Virtual Machine Monitoring (Echo Request - ICMPv6-In)	False	Inbound	Allow
Core Networking - Multicast Listener Report (ICMPv6-Out)	True	Outbound	Allow
Core Networking - Packet Too Big (ICMPv6-In)	True	Inbound	Allow
Core Networking - Multicast Listener Done (ICMPv6-In)	True	Inbound	Allow
Core Networking - Destination Unreachable (ICMPv6-In)	True	Inbound	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	True	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-Out)	True	Outbound	Allow
Core Networking - Neighbor Discovery Solicitation (ICMPv6-Out)	True	Outbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-Out)	False	Outbound	Allow
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	True	Inbound	Allow
Core Networking - Multicast Listener Query (ICMPv6-In)	True	Inbound	Allow
Core Networking - Multicast Listener Report (ICMPv6-In)	True	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)	True	Inbound	Allow
Core Networking - Time Exceeded (ICMPv6-In)	True	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)	True	Inbound	Allow
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)	False	Inbound	Allow
Allow ICMP Inbound	True	Inbound	Allow
Allow ICMP Outbound	True	Outbound	Allow
Active Directory Domain Controller - Echo Request (ICMPv4-Out)	True	Outbound	Allow
Active Directory Domain Controller - Echo Request (ICMPv6-Out)	True	Outbound	Allow

Figure 11: Windows Firewall - ICMP Inbound and Outbound Rules Configured and Enabled

S-DC [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Administrator: Windows PowerShell

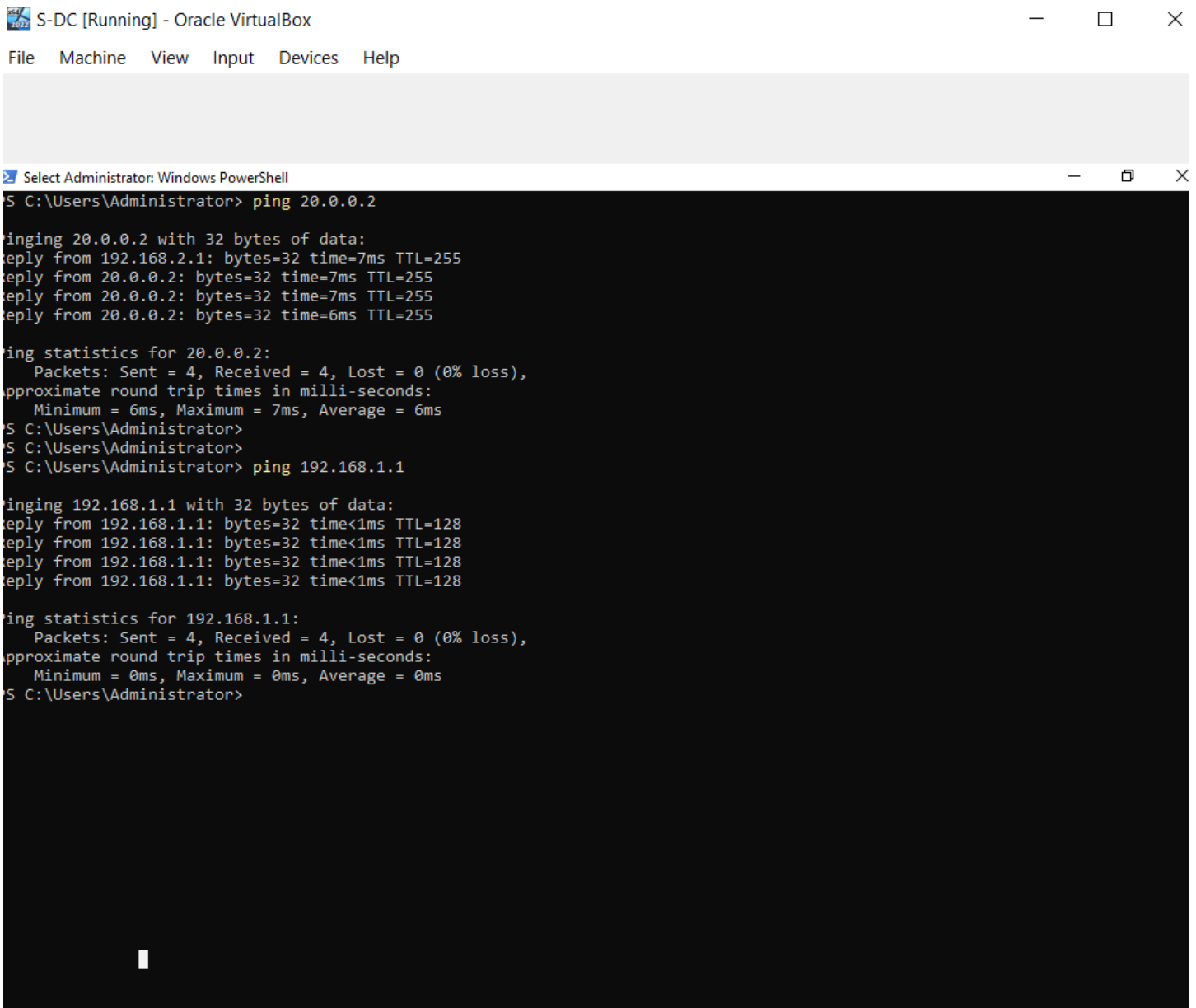
```
Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)      False   Inbound   Allow
Allow ICMP Inbound                                             True    Inbound   Allow
Allow ICMP Outbound                                            True    Outbound  Allow
Active Directory Domain Controller - Echo Request (ICMPv4-Out)  True    Outbound  Allow
Active Directory Domain Controller - Echo Request (ICMPv6-Out)  True    Outbound  Allow
Active Directory Domain Controller - Echo Request (ICMPv4-In)   True    Inbound   Allow
Active Directory Domain Controller - Echo Request (ICMPv6-In)   True    Inbound   Allow

fDenyTSConnections : 0
PSPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal
                    Server
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName         : Terminal Server
PSDrive             : HKLM
PSProvider          : Microsoft.PowerShell.Core\Registry

Status             : Running
Name               : TermService
DisplayName        : Remote Desktop Services

PS C:\Users\Administrator>
```

Figure I2: PowerShell Verification - fDenyTSConnections=0 and Remote Desktop Services Running



```
S-DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Select Administrator: Windows PowerShell
S C:\Users\Administrator> ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=7ms TTL=255
Reply from 20.0.0.2: bytes=32 time=7ms TTL=255
Reply from 20.0.0.2: bytes=32 time=7ms TTL=255
Reply from 20.0.0.2: bytes=32 time=6ms TTL=255

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 7ms, Average = 6ms
S C:\Users\Administrator>
S C:\Users\Administrator>
S C:\Users\Administrator> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
S C:\Users\Administrator>
```

Figure I3: Network Connectivity Test - Successful Ping Results Between Swansea and London Sites

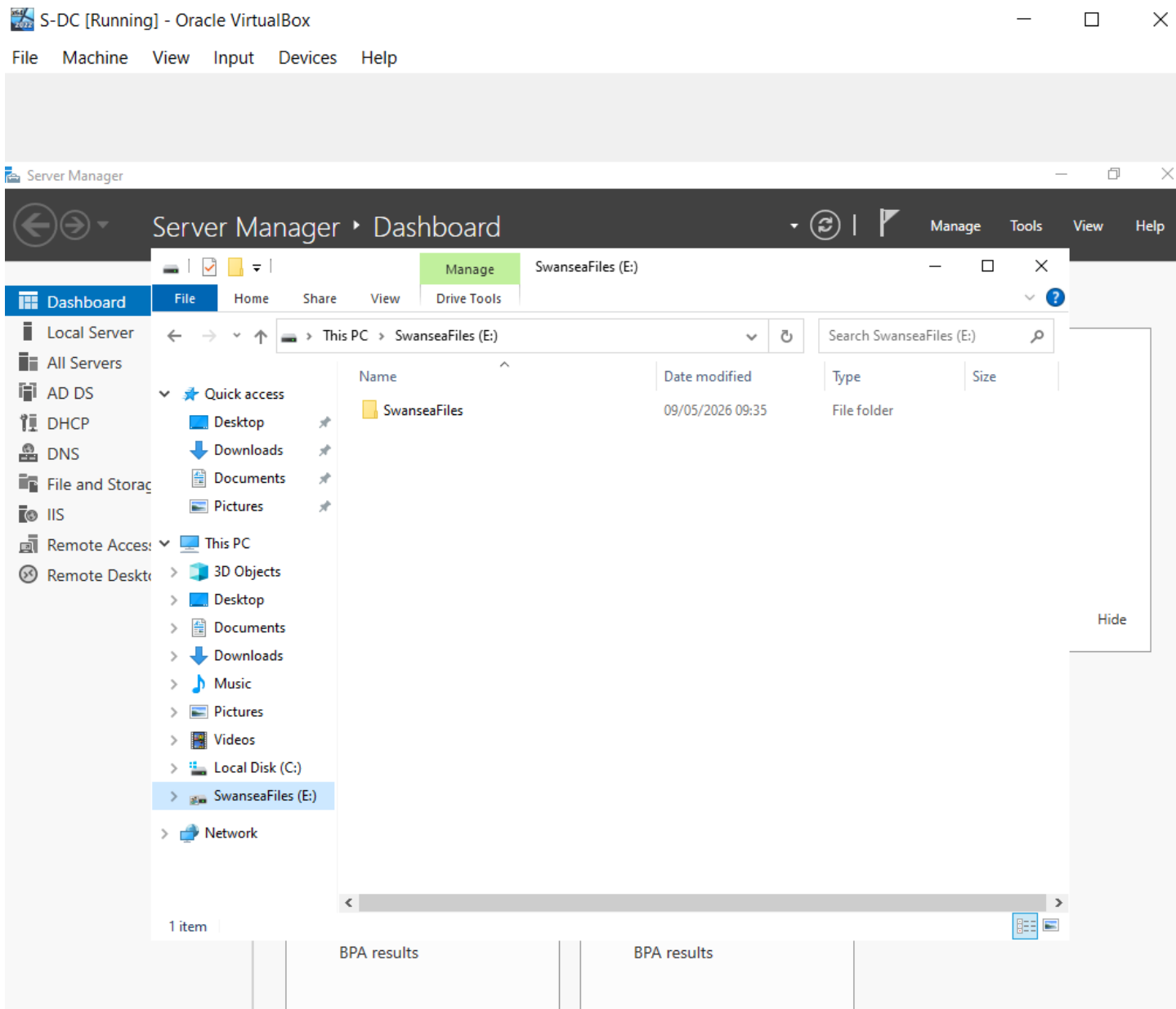


Figure I4: File Explorer - SwanseaFiles Folder Mounted on E: Drive

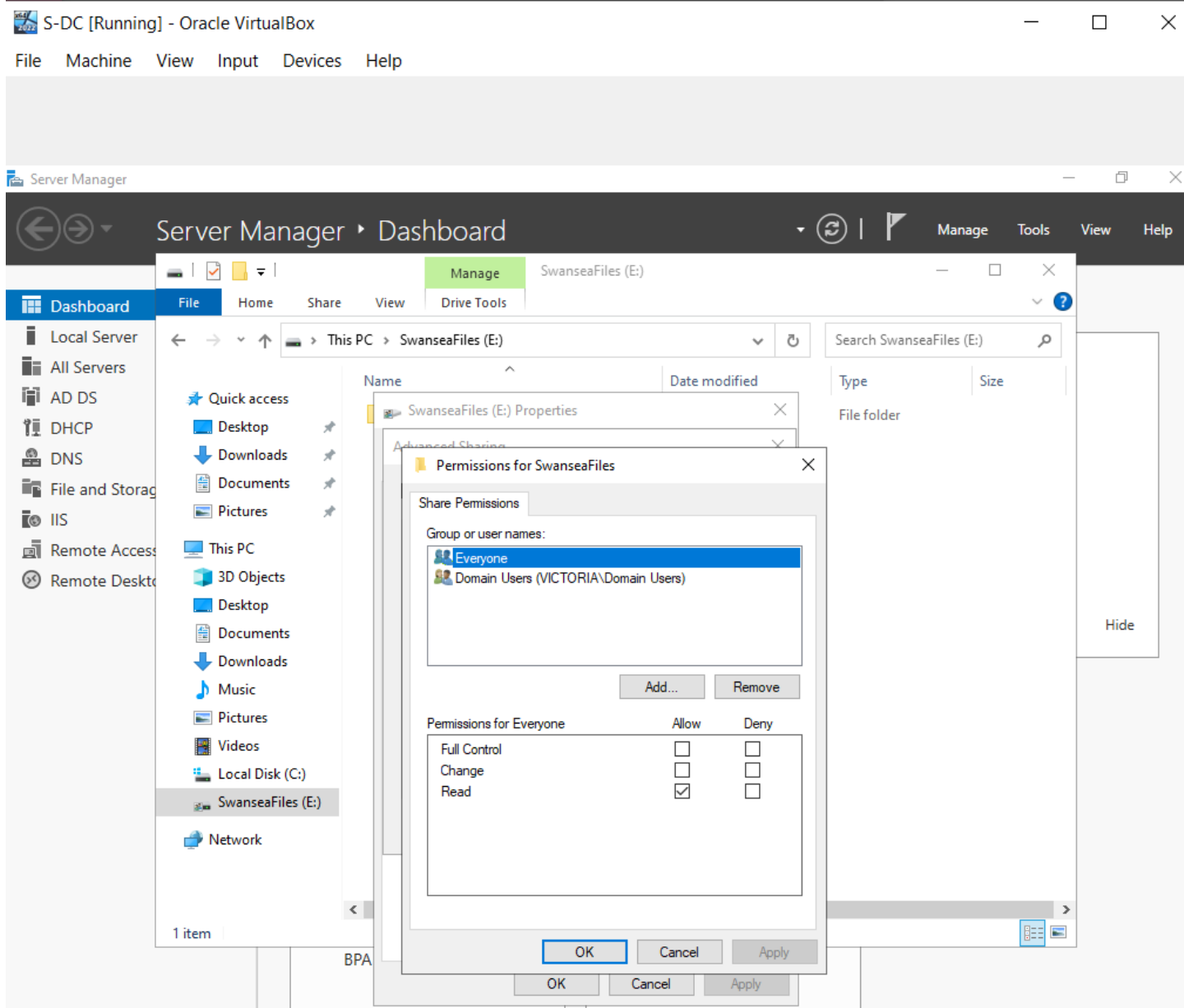


Figure 15: Share Permissions - Everyone Group Configured with Read Only Access

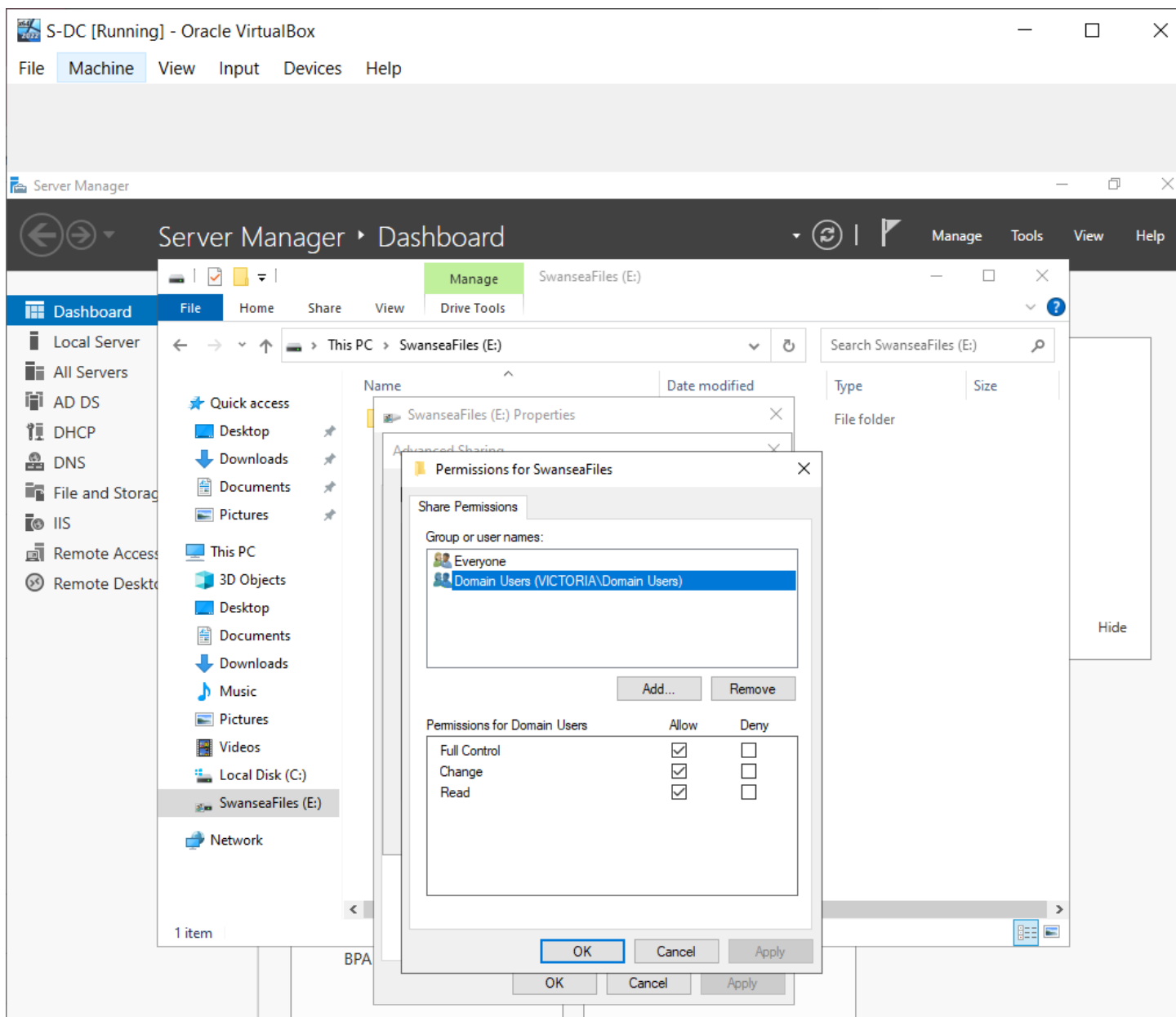


Figure 16: Share Permissions - Domain Users Configured with Full Control Access