Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the** System Checker. The System Checker will confirm that your browser and network connection are ready to support virtual labs.

2. **Review the** Common Lab Tasks document. This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.

3. **When you've finished, use the Disconnect button to end your session and create a StateSave**. To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
   If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.

4. Technical Support **is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
   Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

Security practitioners develop policies, procedures, and controls to help ensure confidentiality, integrity, and availability (CIA). While often considered a part of the system administrator's domain, system availability is very much a security concern. But a complete security program must also include a business impact analysis (BIA). The purpose of this document is to determine the impact to an organization in the event that key processes and technology are not available. The BIA identifies what assets are required for the business to recover from an event and continue doing business. These assets are identified through the risk analysis and assessment process. Risk analysis determines the probability of a risk (such as an earthquake or a power outage) to occur and the impact that occurrence would have on operations. Risk assessment involves a review of controls that could mitigate each risk and weighs the cost, both in terms of time and money, of implementing those controls against the likelihood of the risk itself.

The BIA is the first step in building a business continuity plan (BCP). The BCP creates a plan to continue business after an event. The BCP must clearly define responsibilities and support structures like facilities, personnel, equipment, software, data files, vital records, and contractor and service provider relationships. It should include requirements for downtime for each system. The BCP includes elements such as key assumptions, accountabilities, and how frequently the plan should be tested so that all key personnel are aware of their responsibilities.

Using that information, an organization can develop disaster recovery plans (DRP) for each key system required by the BIA. The DRP documents specific procedures to return a given system or subsystem to production in the event of failure or compromise. The nature of the event determines the amount of recovery effort required. For example, to recover from a short-term power loss, system administrators may need only to reboot the server and perform system checks. However, a much more extensive recovery effort is required if a natural disaster were to damage the facility where those servers are maintained. Global organizations may have to develop several BCPs that are specific to the risks of a given region (including the possibilities of war and terrorism).

In this lab, you will implement a portion of your organization's BCP. Based on the BIA, the organization has determined that the internal Active Directory database and the corporate website must be recoverable in the event of system failure or natural disaster. The BCP recommended that you configure local backups of Active Directory on the existing virtual server using Windows Server Backup. It also suggests that you configure the organization's web servers to host content from a single Network File Share (NFS), and back up that NFS daily using Windows. The BCP has also recommended that these backups are copied to an offsite facility. In the event of a disaster, the DRP includes the procedures necessary to recover the data from the offsite facility and bring the organization's key systems back online.

Learning Objectives

Upon completing this lab, you will be able to:

1. Understand the relationship between business impact analysis, risk analysis, risk assessment, business continuity planning, and disaster recovery planning

2. Install Windows Server Backup and configure a System State backup

3. Configure a Linux NFS server and Linux NFS clients

4. Configure a Windows NFS client

5. Create a backup script and schedule a backup of a remote NFS share

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will install Windows Server Backup.

2. In the second part of the lab, you will configure Windows Server Backup to make a daily backup of Active Directory.

3. In the third part of the lab, you will configure two web servers to use a common NFS share for web content.

4. In the fourth part of the lab, you will configure Windows to back up the common NFS share.

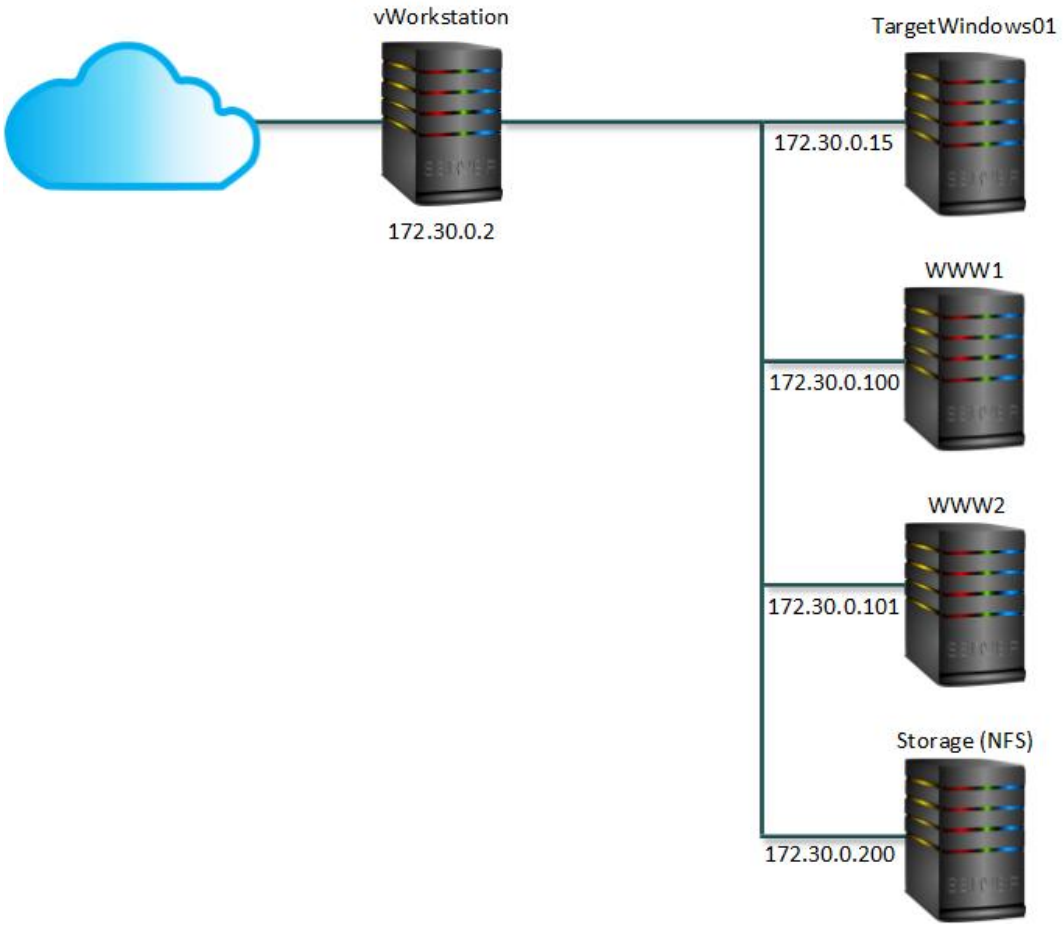
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindows01 (Windows Server 2016)
- www1 (Web Server)
- www2 (Web Server)
- Storage (Network File System Server)



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Nano Editor
- PowerShell
- PuTTY
- Server Manager
- vi Editor
- wbadmin

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- Scheduled Backup configuration and the system clock;
- updated website content for both web servers;
- contents of the Z: directory;
- contents of the c:\www directory;
- contents of the c:\backup directory;

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- scheduled backup settings;
- filesystem mount point for both web servers;
- symbolic link for c:\www;
- contents of the c:\www directory;
- contents of the c:\backup directory;

2. Files downloaded from the virtual environment:

- Backup-datetime.log;
- *yourname*_wwwbackup.bat;

3. Any additional information as directed by the lab:

- none.

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Install Windows Server Backup

Note: In the next steps, you will install the Windows Server Backup and Client for NFS features on a Windows 2016 Server machine using the Server Manager GUI.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.

2. In the Connections folder, **double-click** the **TargetWindows01 RDP shortcut** to open a remote connection to the TargetWindows01 machine.

   If prompted, **type** the following credentials and **click OK**.

   - Username: **`Administrator`**
   - Password: **`P@ssw0rd!`**

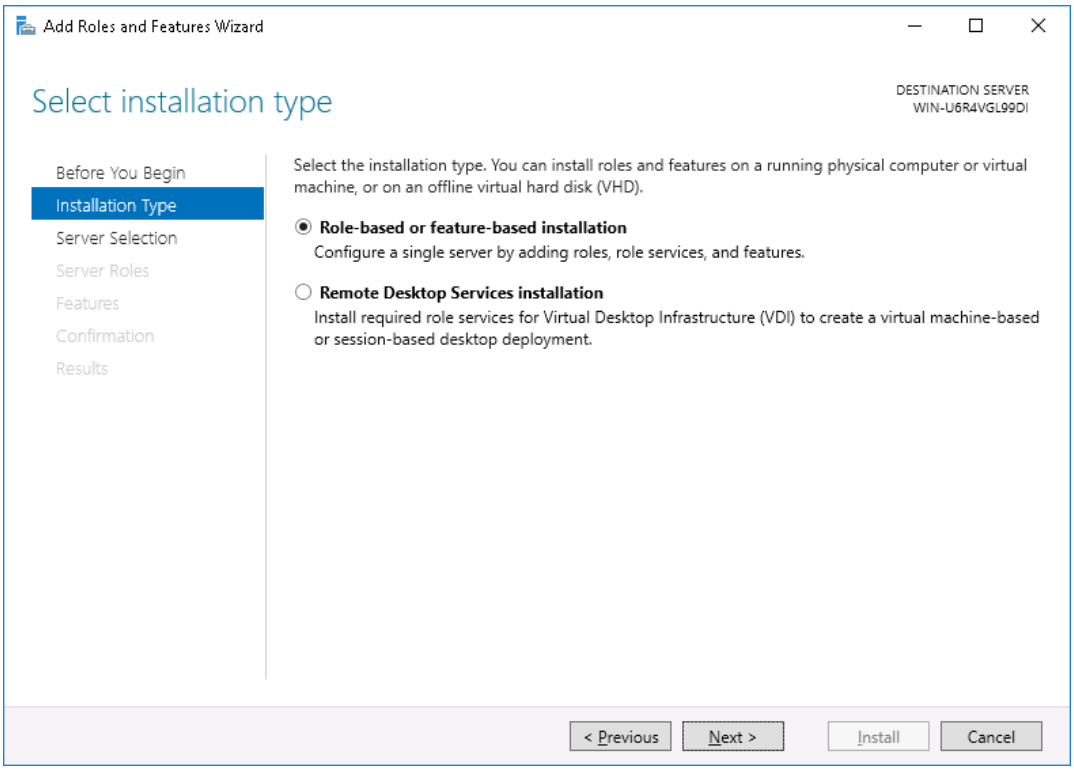
   The remote desktop opens with the IP address of TargetWindows01 (172.30.0.15) in the title bar at the top of the window.

3. On the TargetWindows01 taskbar, click the **Windows Start icon**, then **click** the **Server Manager button** to open the Server Manager application.

4. From the Server Manager menu, **select Manage > Add Roles and Features** to open the Add Roles and Features Wizard.

5. On the Before You Begin page, **click Next** to continue.

6. On the Installation Type page, **select** the **Role-based or feature-based installation option** and **click Next** to continue.



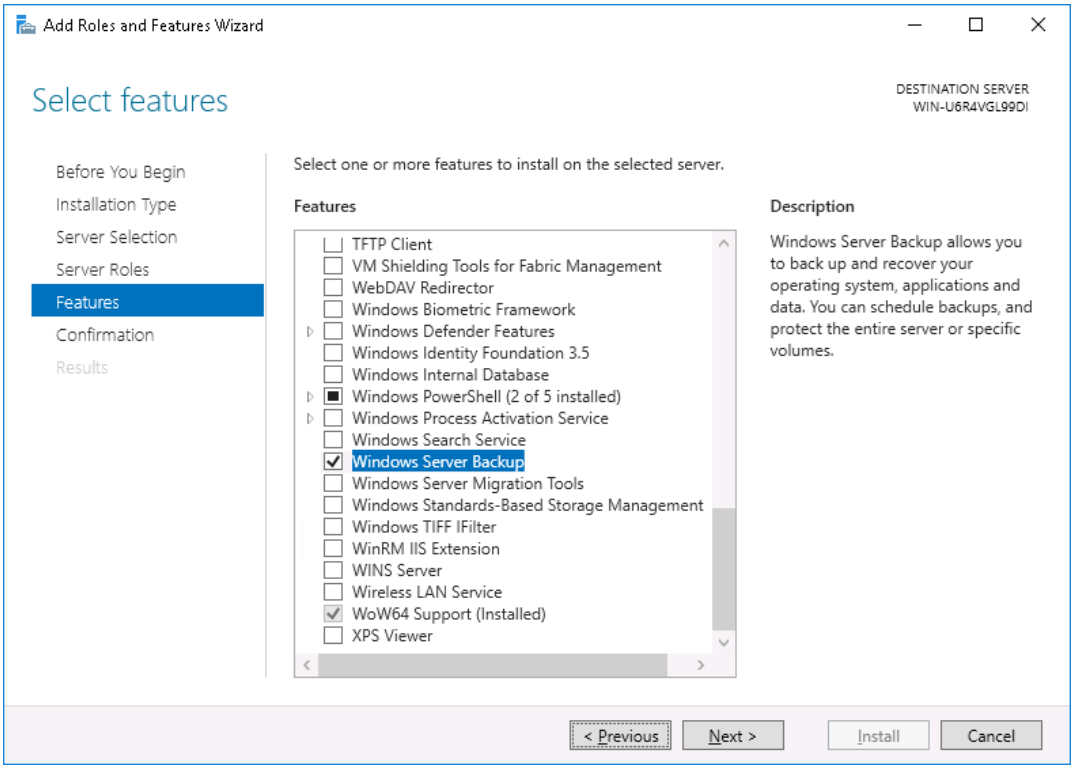
Select installation type page

7. On the Server Selection page, **click Next** to accept the default options.

8. On the Server Roles page, **click Next** to accept the default options.

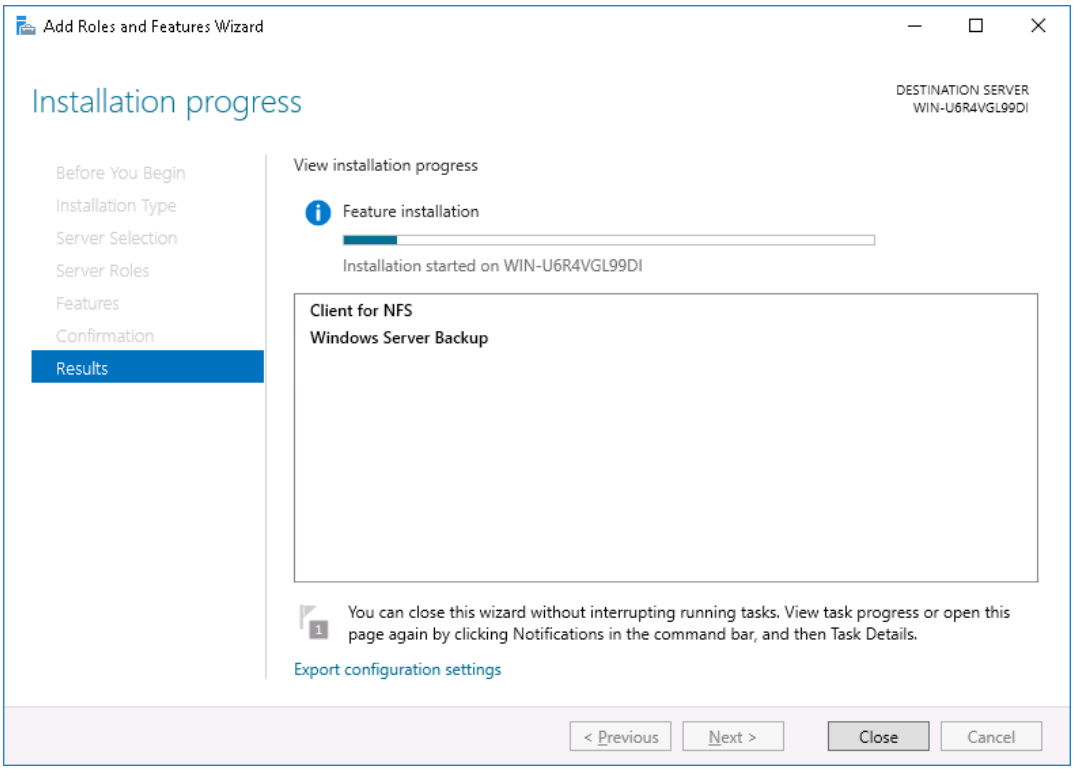
9. On the Features page, **click** the **Client for NFS checkbox** to enable the computer to access files on UNIX-based NFS servers.

10. On the Features page, **click** the **Windows Server Backup checkbox** to allow you to backup and recover data, then **click Next** to continue.



Select features to install

11. On the Confirmation page, **click Install** to install the selected features.



Installation progress

12. When the installation is completed, **click Close** to close the Add Roles and Features Wizard.

Part 2: Configure (System State) Backup

Note: In the next steps, you will use Windows Server Backup to make a daily backup of System State. This same process will be used for Active Directory servers. (Active Directory contains all of the users, groups, distribution lists, and organizational units used in the Domain.)

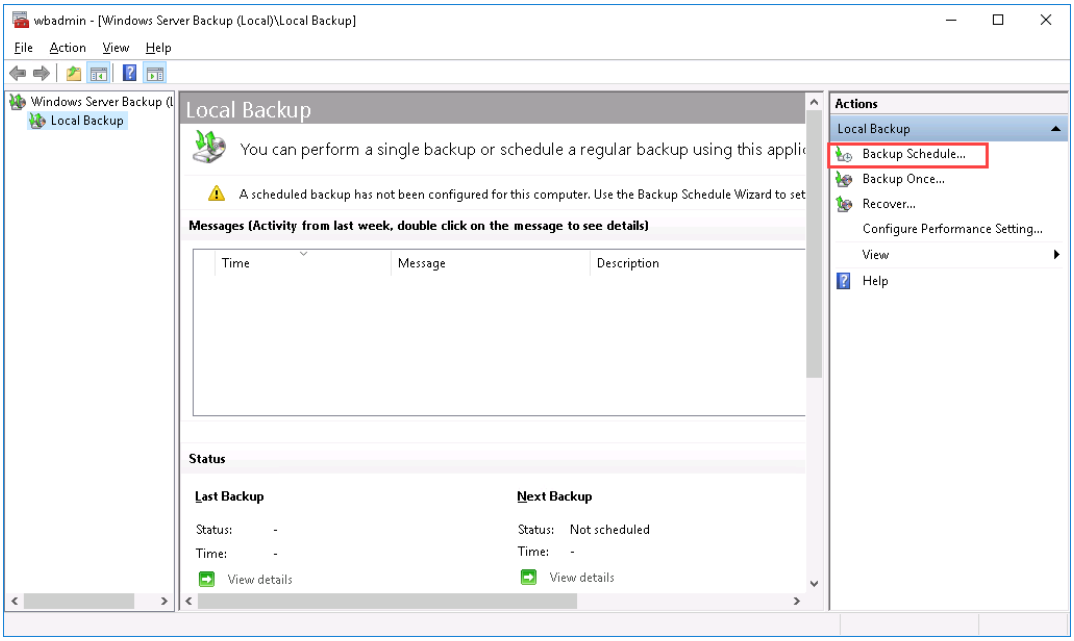
1. From the Server Manager menu, **select Tools > Windows Server Backup** to open the Windows Backup Admin (wbadmin).

2. In the left pane of the wbadmin, **click Local Backup** to select the Local Backup option.

   You should see an amber caution sign in the center pane indicating that there is no backup

currently scheduled.

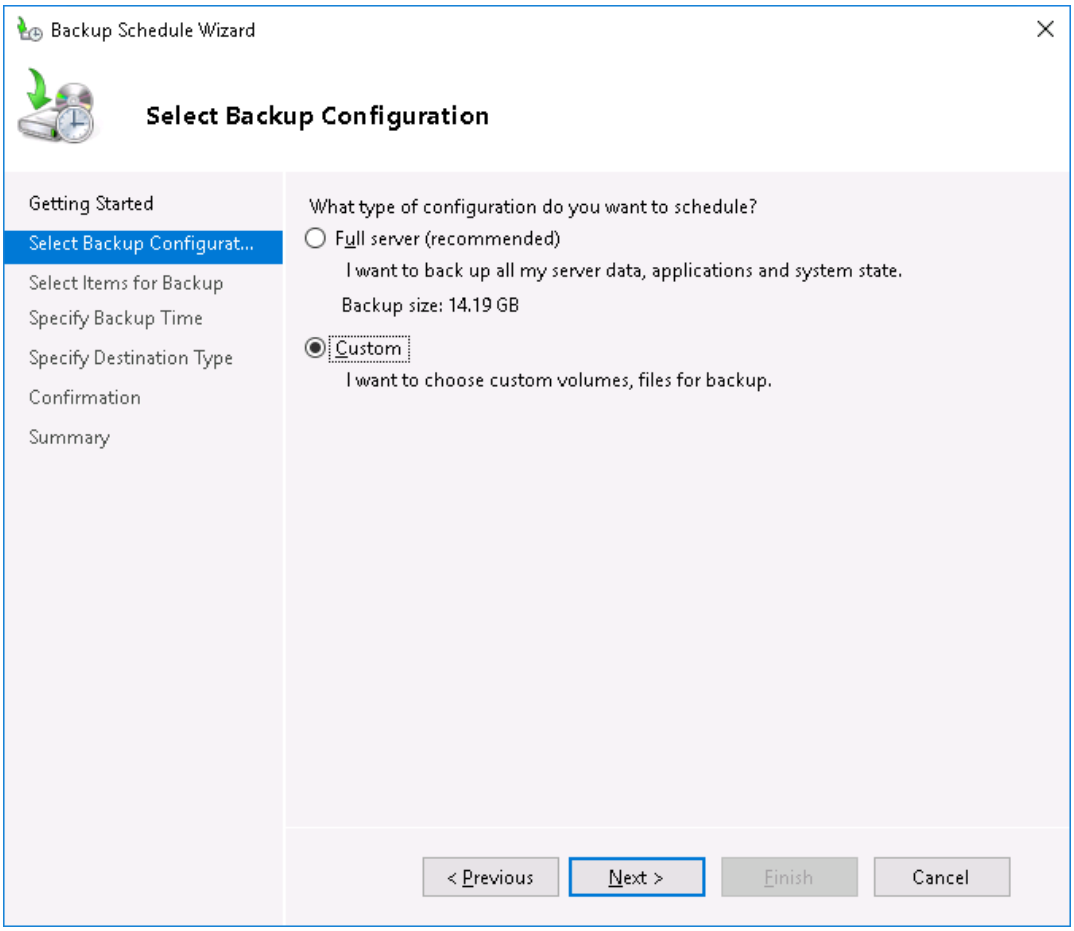
3. In the right pane of the wbadmin, **click Backup Schedule** to launch the Backup Schedule wizard.



Backup Schedule pane

4. On the Getting Started page, **click Next** to continue.

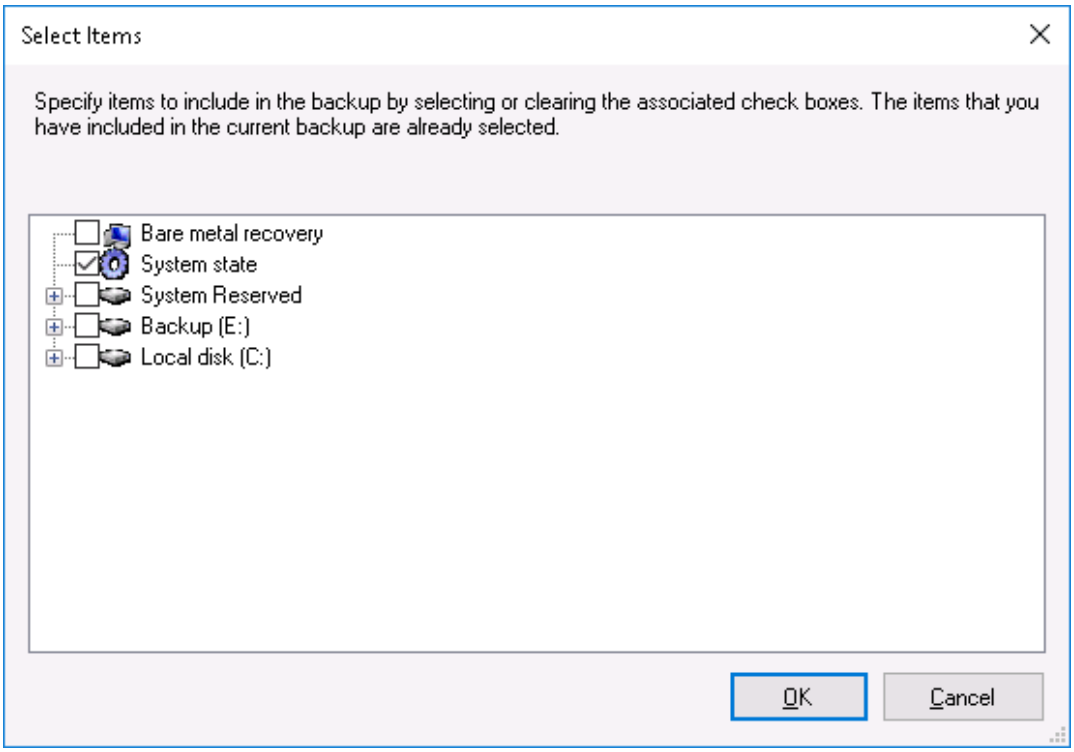
5. On the Select Backup Configuration page, **click** the **Custom radio button** to select a custom backup configuration, then **click Next** to continue.



Select Backup Configuration page

6. On the Select Items for Backup page, **click Add Items** to open the Select Items dialog box.

7. In the Select Items dialog box, **click** the **System state checkbox** and **click OK**.



Select items to back up

8. On the Select Items for Backup page, **click Next** to continue.

Note: In the following step, you will enter a time that corresponds with the system time on your lab session *plus 6 hours*. For example: If the system time on your lab session is 2:30 PM, select 8:30 PM as the time for the backup. The Select Time of Day drop-down menu lists times in ½ hour increments. Round your time to the nearest 30 minute interval.

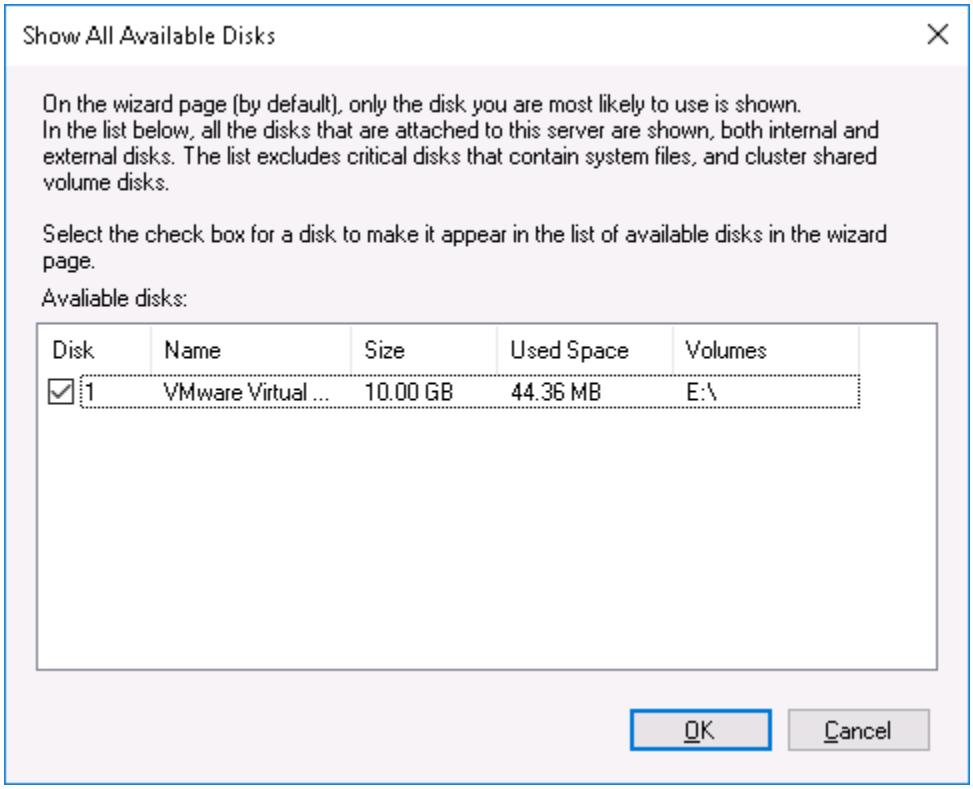
9. On the Specify Backup Time page, **click** the **Once a day radio button**, **click** the **Select time of day drop-down menu**, and **select a time that corresponds to 6 hours from the current system time**.

10. On the Specify Backup Time page, **click Next** to continue.

11. On the Specify Destination Type page, **click Next** to accept the default option and continue.

12. On the Select Destination Disk page, **click Show All Available Disks** to open the Show All Available Disks dialog box.

13. In the Show All Available Disks dialog box, **click** the **10GB drive checkbox** and **click OK** to add this option to the Select Destination Disk page.

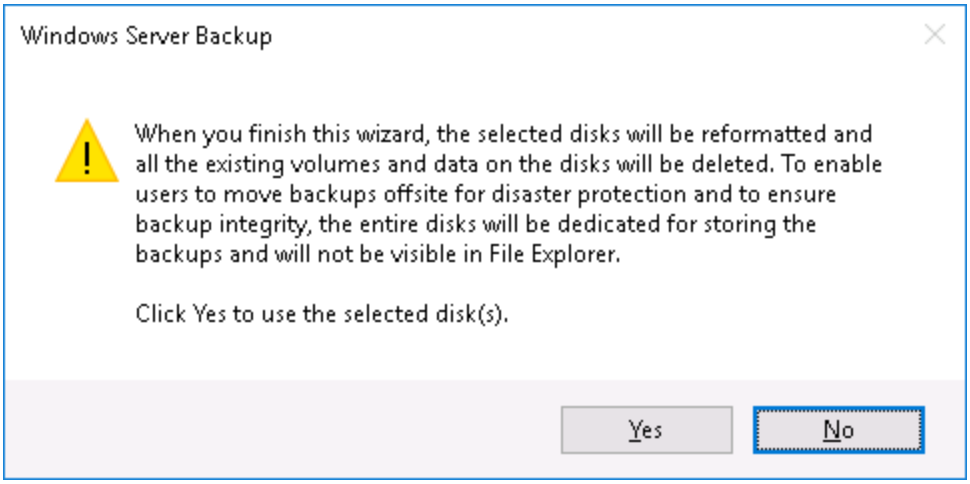


Select dedicated drive

Note: If your drive is too small in size, Windows will force the drive offline, making it unusable.

14. On the Select Destination Disk page, **click** the **10GB drive checkbox** and **click Next** to confirm the selection.

    The system will generate a notice that the selected disk will be reformatted.



Confirmation pop-up

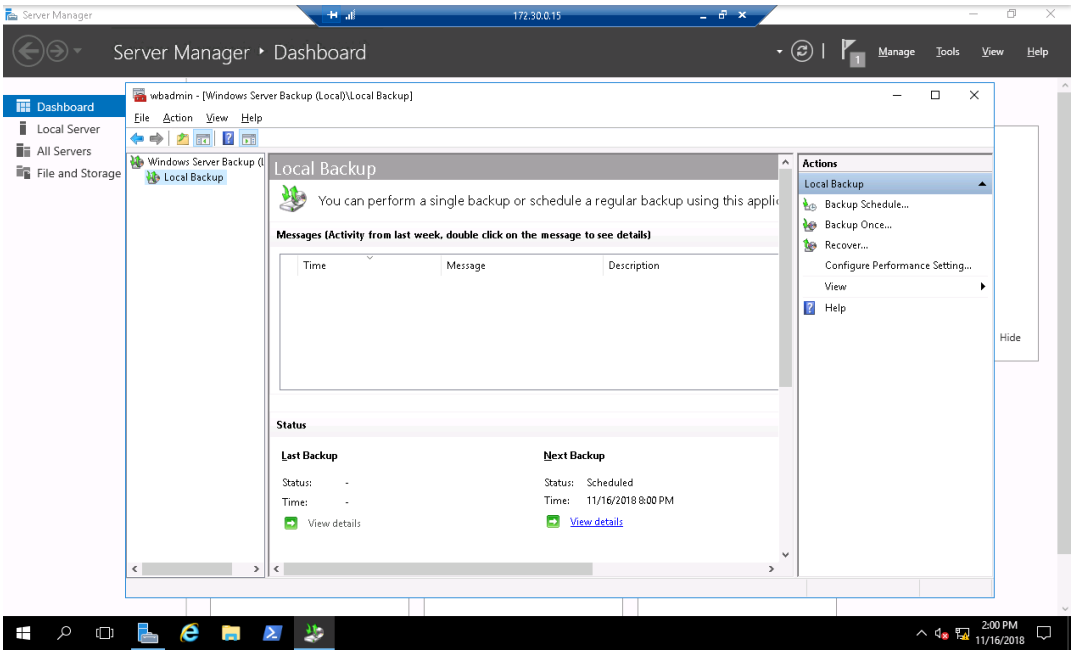
15. **Click Yes** to close the confirmation pop-up, then **click Finish** to continue.

    The backup schedule wizard will configure your selections and display a summary page confirming the time of the first scheduled backup.

16. On the Summary page, **click Close** to close the Backup Schedule Wizard.

    The wbadmin window will display the next scheduled backup time in the center pane.

17. In the wbadmin, **use the scrollbar** to display the scheduled backup configuration, as shown in the following figure.



Scheduled backup with system clock

18. **Make a screen capture** showing the **Scheduled Backup configuration and the system clock** and **paste** it into your Lab Report file.

19. **Close** any **open windows**.

20. **Minimize** the **remote TargetWindows01 connection**.

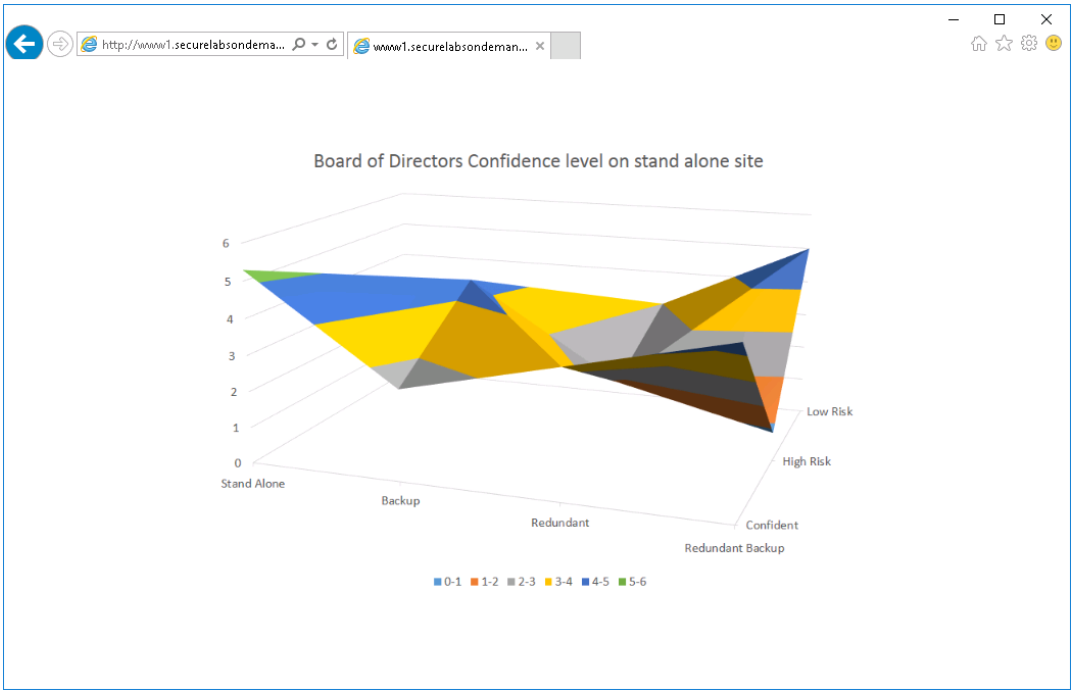
Part 3: Configure Websites to use a Common NFS Share

Note: In this part of the lab, you will configure redundant web servers (www1 and www2) to use a Network File System (NFS) on a third storage server for web content. Originally used in the UNIX operating system, an NFS is used to make remote folders appear as part of the local file system on Linux and even Windows systems.

1. On the vWorkstation taskbar, **click** the **Internet Explorer icon** to open a new Internet Explorer window.

2. In the address box, **type** `http://www.securelabsondemand.com` and **press Enter** to view the content of the master default web page.

3. In the address box, **type** `http://www1.securelabsondemand.com` and **press Enter** to view the content of the default web page for this URL.



Web content on www1

4. In the address box of the browser, **type** `http://www2.securelabsondemand.com` and **press Enter** to view the content of the default web page for this URL.

   You will notice that the content of the default web page is different on each website. In the next steps, you will configure the www1 and www2 sites to become a redundant version of the master www website.

5. **Close** the **Internet Explorer window**.

6. In the Connections folder, **double-click** the **storage shortcut** to open a PuTTY session to the Storage server.

7. At the command prompt, **type** `cd /etc` and **press Enter** to change the directory.

8. At the command prompt, **type** `vi exports` and **press Enter** to open the exports file in the vi Editor.

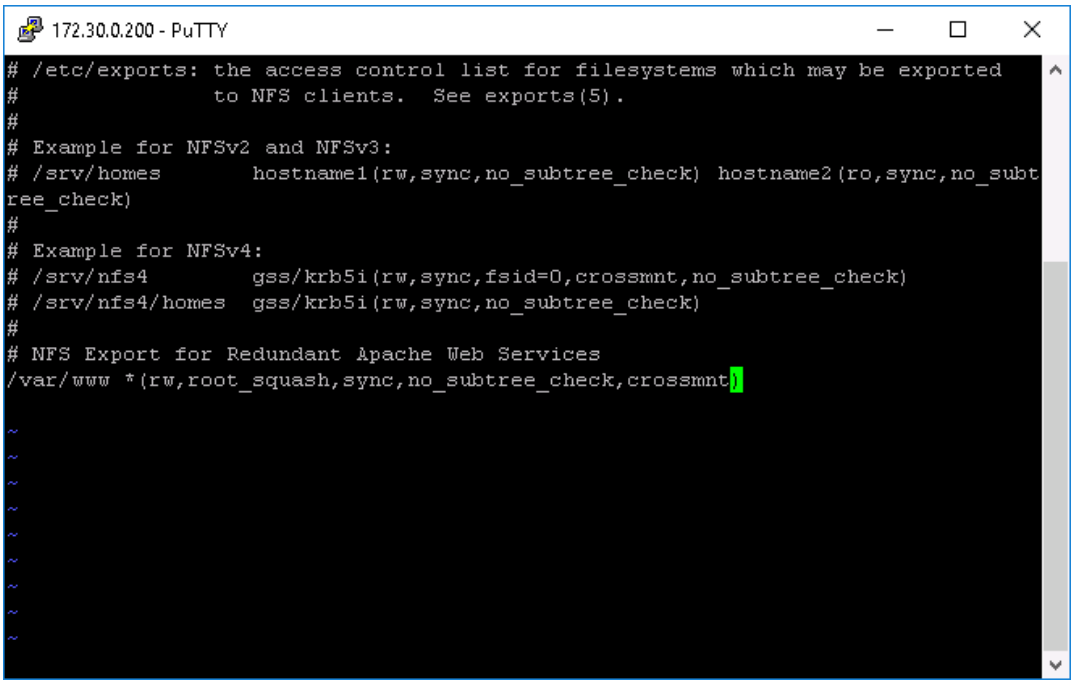
   The vi Editor (visual editor) is a UNIX screen editor.

Note: The /etc/exports file instructs Linux which folders to share with NFS and what NFS features should be enabled. In the next steps, you will add a new line of code that instructs Linux to share /var/www. The options used in the /var/www command are described in the following list.

- The asterisk (`*`) is a wild card, any IP may connect.
- `rw` grants read write access.
- `root_squash` prevents root from creating files with root privilege.
- `sync` synchronizes local and remote directories.
- `no_subtree_check` will not export sub directories.
- `crossmnt` allows multiple client mounts and multi filesystem mounting

9. In the vi Editor, **use** the **down arrow** to position the cursor at the last line of text, then **press o** to add a new line and open edit mode.

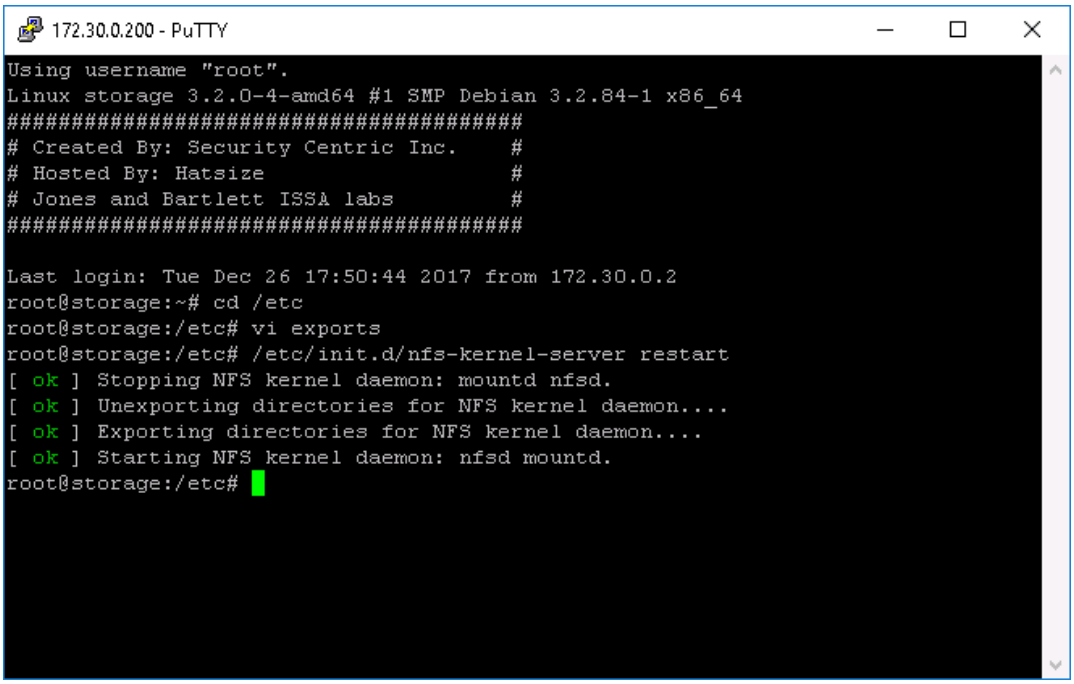
10. At the new line, **type** `/var/www *(rw,root_squash,sync,no_subtree_check,crossmnt)`, then **press Esc** to exit edit mode.



Edit exports in vi Editor

11. In the vi Editor, **type** `:wq!` and **press Enter** to save the changes and exit the vi Editor.

12. At the command prompt, **type** `/etc/init.d/nfs-kernel-server restart` and **press Enter** to restart the NFS server on storage.securelabsondemand.com.



Restart NFS

13. At the command prompt, **type** `exit` and **press Enter** to close the PuTTY session.

14. In the Connections folder, **double-click** the **www1 shortcut** to open a new PuTTY session to the www1 server.

15. At the command prompt, **type** `cd /etc` and **press Enter** to change the directory.

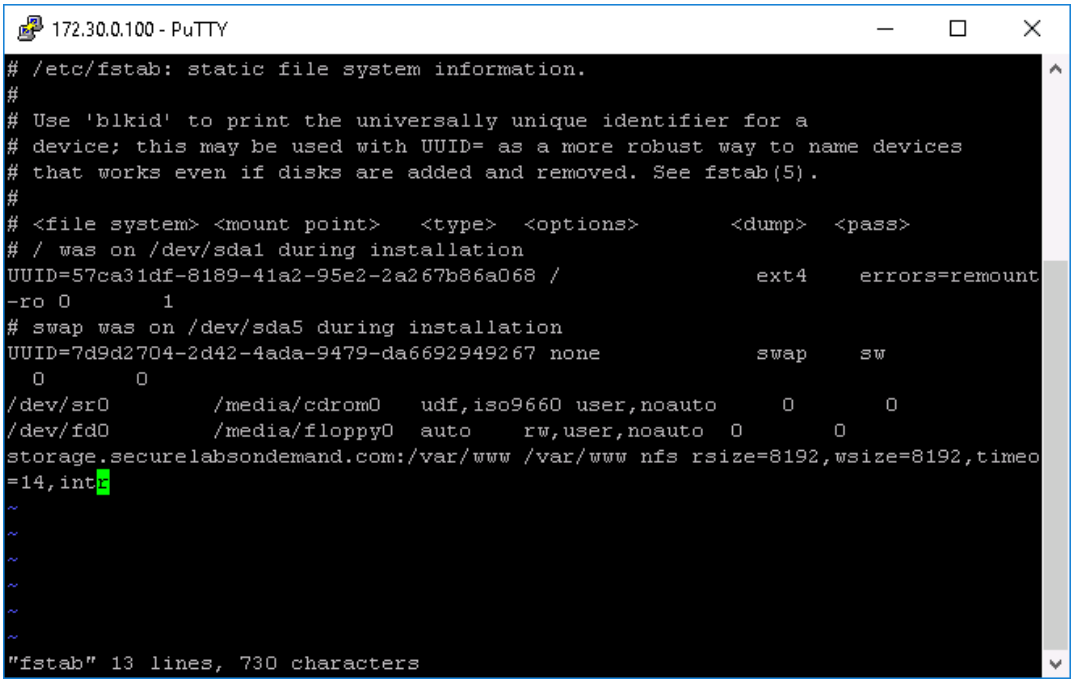
16. At the prompt, **type** `vi fstab` and **press Enter** to open the file systems table in the vi Editor.

Note: The /etc/fstab instructs the Linux system which files to mount on startup. In the next steps, you will add a line that instructs www1 to mount the /var/www directory, which you “exported” in the PuTTY session to the Storage server.

17. In the vi Editor, **use** the **down arrow** to position the cursor at the last line of text, then **press o**

to add a new line and open edit mode.

18. At the new line, **type** `storage.securelabsondemand.com:/var/www /var/www nfs rsize=8192,wsize=8192,timeo=14,intr`, then **press Esc** to exit edit mode.

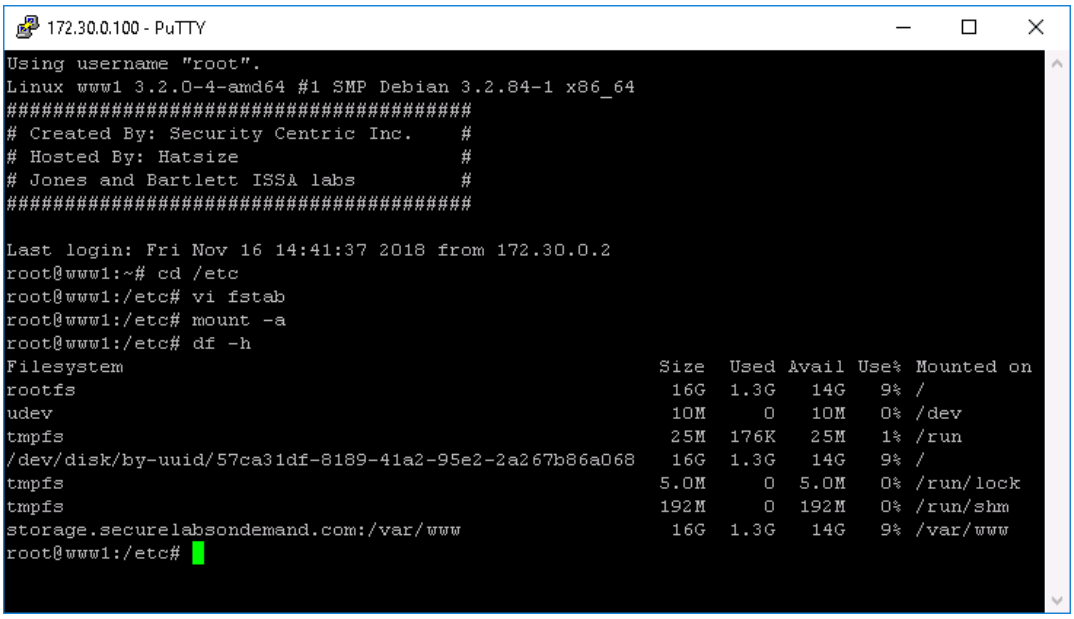


Edit fstab in vi editor

19. In the vi Editor, **type** `:wq!` and **press Enter** to save the changes and exit the vi Editor.

20. At the command prompt, **type** `mount -a` and **press Enter** to mount the storage server.

21. At the command prompt, **type** `df -h` and **press Enter** to verify that the storage server has been mounted correctly.



Display the file system

22. At the command prompt, **type** `exit` and **press Enter** to close the PuTTY session.

23. In the Connections folder, **double-click** the **www2 shortcut** to open a PuTTY session to the www2 server.

24. **Repeat steps 15-22** for the www2 server (172.30.0.101).

Note: You have now configured both www1 and www2 to use the same NFS folder on the storage server. In the next steps, you will confirm that your changes have taken place.

25. On the vWorkstation taskbar, **click** the **Internet Explorer icon** to open a new Internet Explorer window.

26. In the address box, **type** `http://www.securelabsondemand.com` and **press Enter** to view the content of the master default web page.

27. In the address box, **type** `http://www1.securelabsondemand.com` and **press Enter** to view the content of the default web page.

    You will see updated web content hosted on the common NFS mount (/var/www on storage). If you do not see new content, **refresh** the **web page**.

28. **Make a screen capture** showing the **updated website content** and **paste** it into your Lab Report file.

29. **Repeat steps 27-28** for the http://www2.securelabsondemand.com site.

30. **Close** the **Internet Explorer window**.

Part 4: Use Windows to Back Up the Common NFS Share

Note: In the next steps, you will configure TargetWindows01 to automatically back up the /var/www NFS share on the storage server. You will begin with the *mount* command. The command and the options used are described below:

```
mount -o mtype=hard 172.30.0.200:/var/www *
```

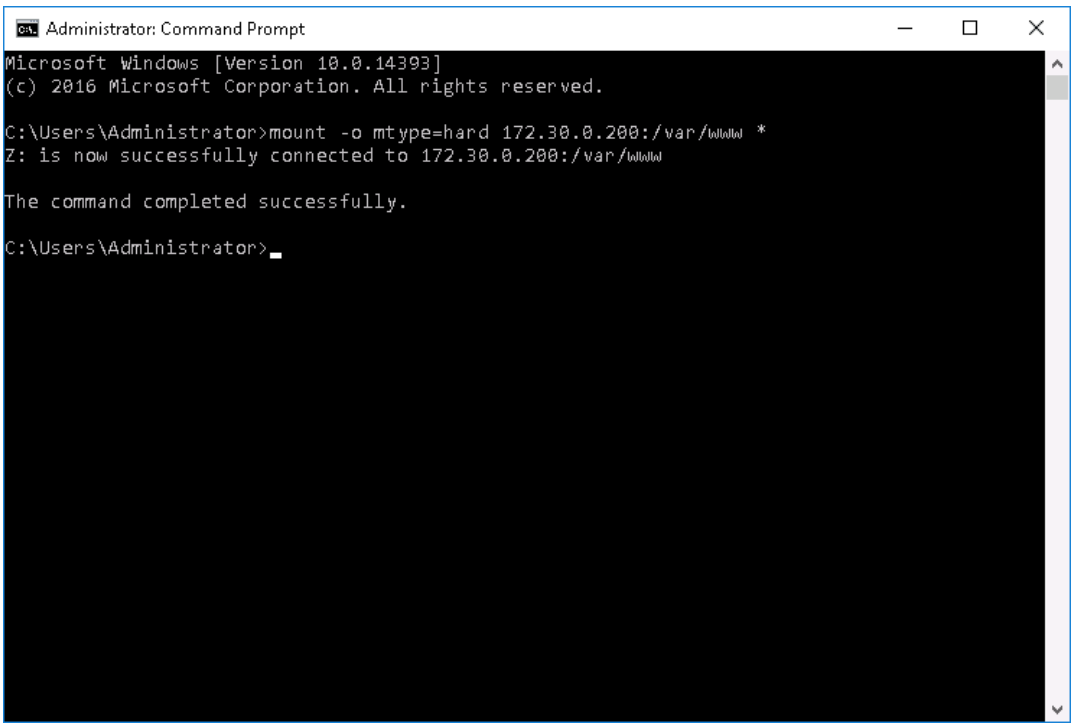
- `mount` attaches the file system
- `-o` introduces a list of options
- `mtype` can be specified as hard or soft
  - (Hard: Will attempt to reconnect to the NFS without errors if the NFS becomes unavailable)
  - (Soft: Will attempt to reconnect to the NFS but will report an error if NFS is unavailable)
- `172.30.0.200:/var/www` is the IP address and path that will be shared
- `*` (the asterisk) is a wildcard that directs the command to use any available drive letter for the new share

1. **Restore** the **remote TargetWindows01 connection**.

2. On the TargetWindows01 taskbar, **right-click** the **Windows Start menu**, then **select Command Prompt** to open a new command prompt window.

3. At the command prompt, **type** `mount -o mtype=hard 172.30.0.200:/var/www *` and **press Enter** to mount /var/www on storage.securelabsondemand.com to the next available

drive on TargetWindows01.



NFS mount command

4. At the command prompt, **type** `dir z:` (the directory found in step 3) to change the directory and read the contents of the web server (2 files and 3 directories).

5. **Make a screen capture** showing the **contents of the Z: directory** and **paste** it into your Lab Report file.

6. At the command prompt, **type** `mklink /D c:\www z:` and **press Enter** to create the share folder.

Note: The mklink command creates a symbolic link so that remote Z: drive can be accessed as a local folder called www on the C: drive. This type of link enables tools like xcopy to work on remote drives by making them appear local to the OS.

7. At the command prompt, **type** `cd \` and **press Enter** to change to the root directory.

8. At the command prompt, **type** `cd www` and **press Enter** to change directories to the new linked directory.

9. At the command prompt, **type** `dir` and **press Enter** to list the files in the new linked directory.

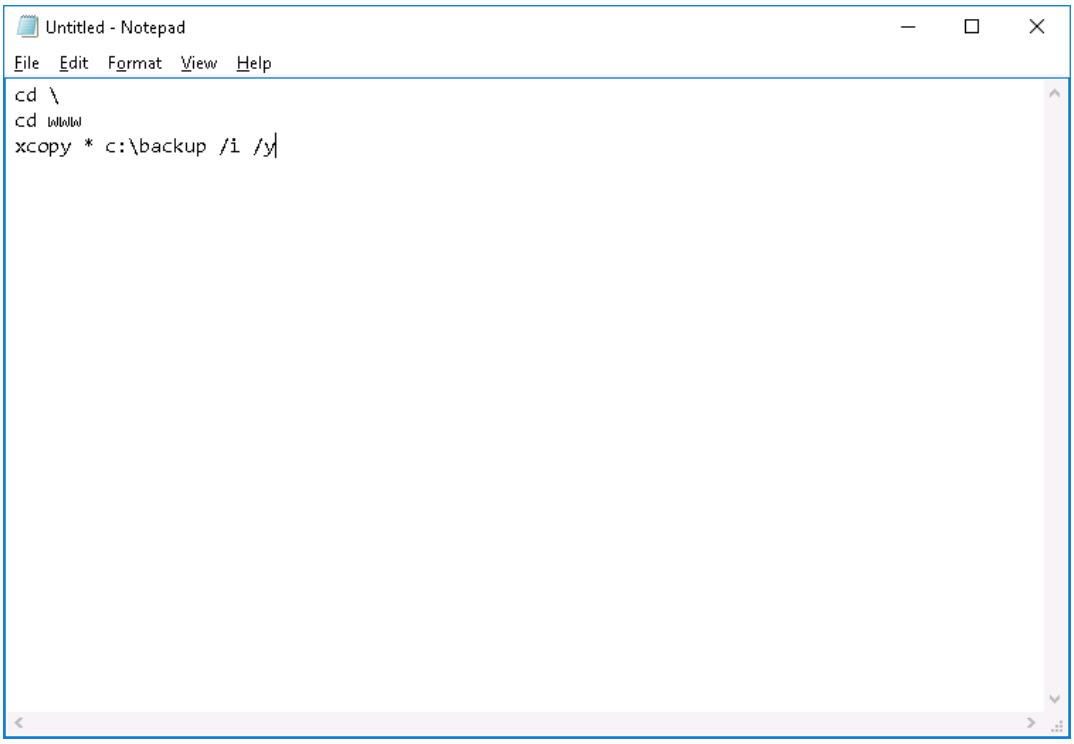
10. **Make a screen capture** showing the **contents of the www directory** and **paste** it into Lab Report file.

Note: In the next steps, you will create a batch file. A batch file is a text file containing a series of commands that the computer should execute. First, you will create the text file to use xcopy to create a backup copy of the new www folder (creating a new backup folder when necessary and overwriting existing files each time the command is run), and then you will schedule that backup command to recur every day.

11. At the command prompt, **type** `notepad` and **press Enter** to open a Notepad window.

12. In the Notepad window, **type** the following lines of text.

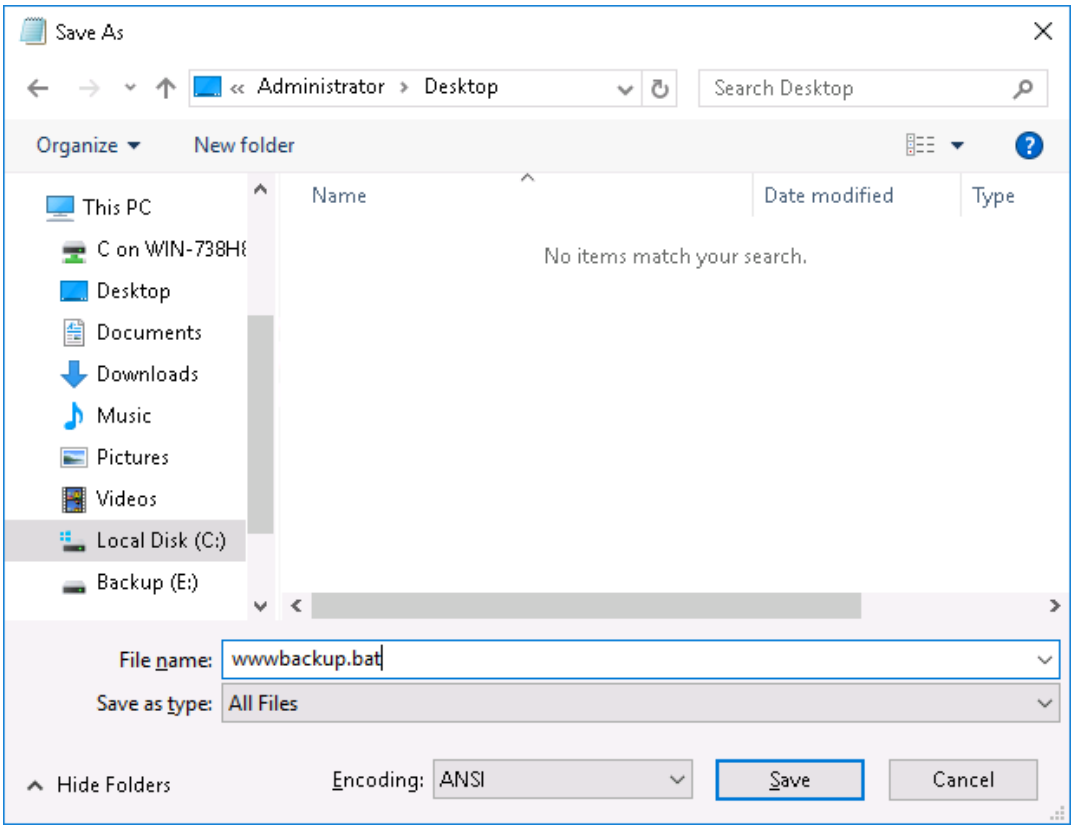
```
cd \
cd www
xcopy * c:\backup /i /y
```



Create the batch file

13. From the Notepad menu bar, **select File > Save as** to open the Save As dialog box.

14. In the Save As dialog box, **navigate** to the TargetWindows01 desktop (**C:\Users\Administrator\Desktop**), then **type** `wwwbackup.bat` in the File name box, **select All Files** in the Save as type box, and **click Save** to save the Notepad file as a batch file on the TargetWindows01 desktop.



Save the batch file

15. **Close** the **Notepad window**.

16. At the command prompt, **type** `schtasks /create /tn "Web Backup" /tr C:\Users\Administrator\Desktop\wwwbackup.bat /sc daily` and **press Enter** to create a new task named Web Backup and schedule that task to run the batch file you created on a daily basis.

    Note that the capitalization is important for this command to function properly. The system will then ask you to replace the existing Web Backup file; **type** `Y` and **press Enter** to schedule the new task.

17. At the command prompt, **type** `schtasks /run /tn "Web Backup"` and **press Enter** to run the scheduled task immediately.

If prompted to overwrite a file, **type** `Y` to continue.

18. At the command prompt, **type** `dir c:\backup` and **press Enter** to verify that the Web Backup task copied the files from the www directory.

19. **Make a screen capture** showing the **contents of the c:\backup directory** and **paste** it into your Lab Report file.

20. At the command prompt, **type** `exit` and **press Enter** to close the Command Prompt window.

Note: This completes Section 1 of this lab. There are no deliverable files for this section.

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
   a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.

   b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.

3. **Proceed** with **Part 1**.

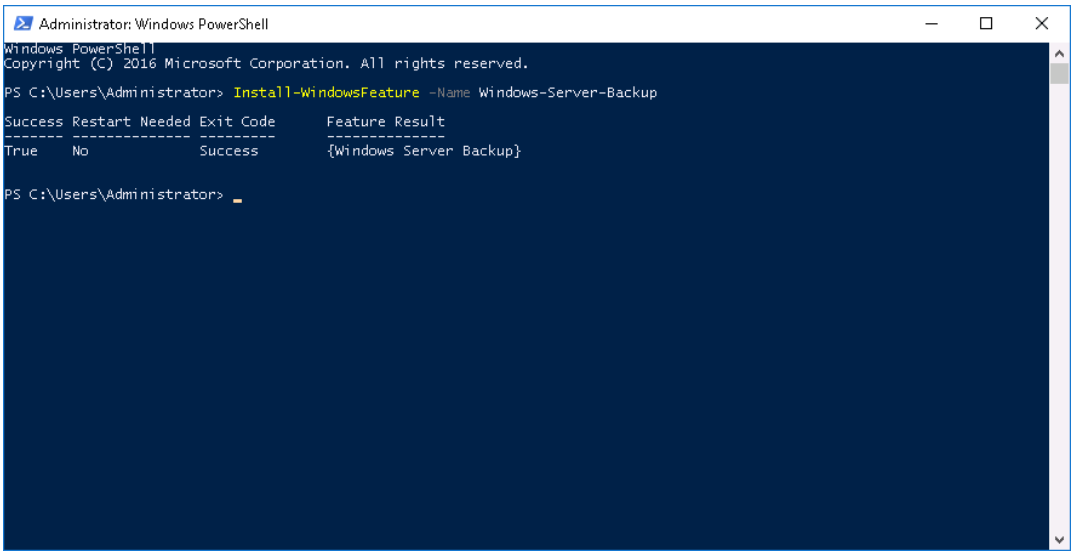
Part 1: Install Windows Server Backup and NFS-Client

Note: In the next steps, you will install the Windows Server backup and NFS client features on a Windows 2016 Server using a mix of PowerShell and CMDLET commands.

1. **Open a remote connection** to the **TargetWindows01** machine.

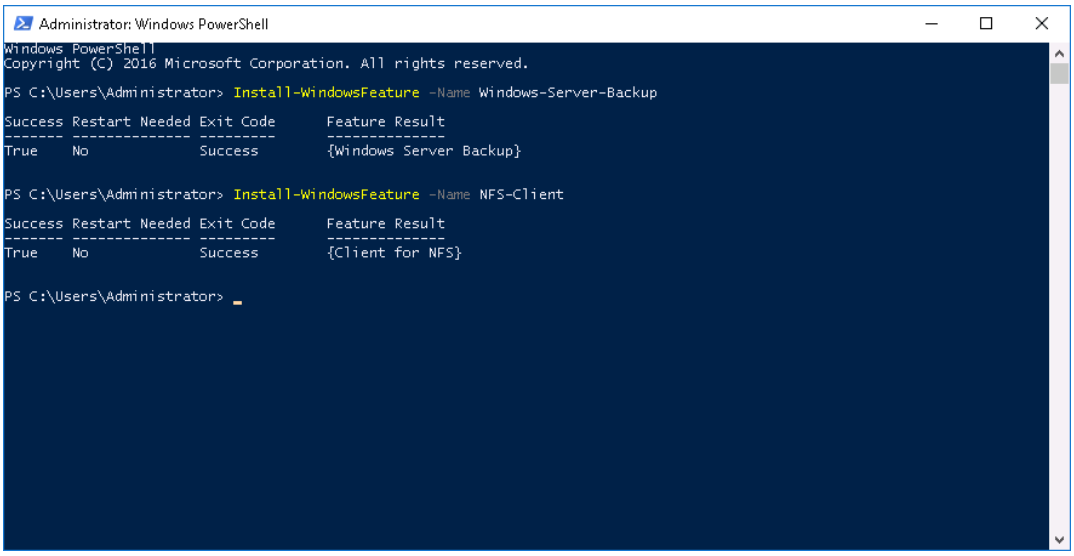
2. From the TargetWindows01 taskbar, **launch Windows PowerShell**.

3. At the PowerShell prompt, **execute `Install-WindowsFeature -Name Windows-Server-Backup`** to install the Windows Server Backup feature.



Successful Windows Server Backup installation

4. At the PowerShell prompt, **execute `Install-WindowsFeature -Name NFS-Client`** to install the NFS-Client feature.



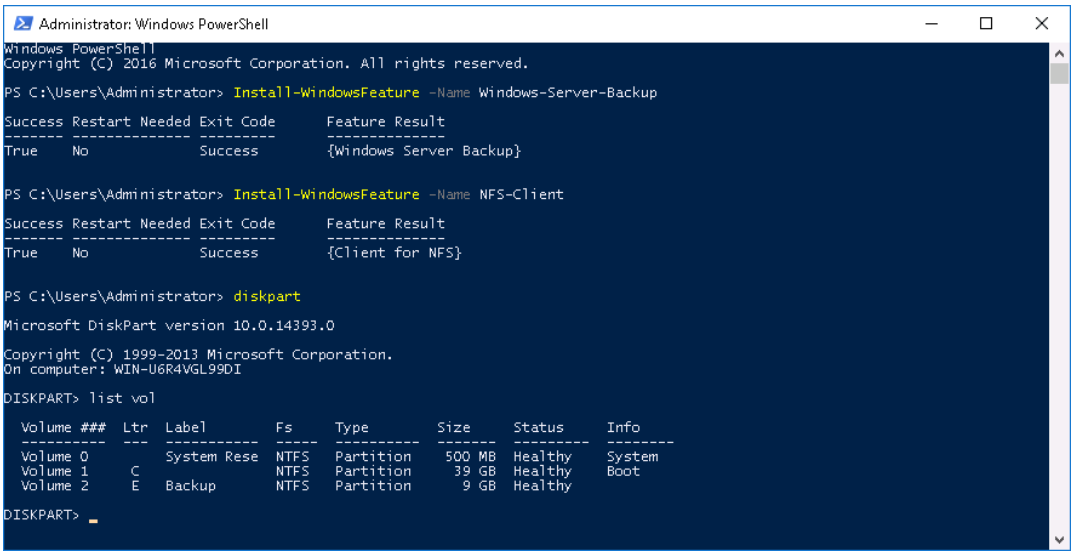
Successful Client for NFS installation

Note: Diskpart is a text-mode command interpreter in Windows Server 2016. This tool enables you to manage objects (disks, partitions, or volumes) by direct input at the command line. With diskpart you can expand disk space dynamically on the fly with active drives. (Expanding drive space can only be done if the space is already existing and unallocated space).

5. At the PowerShell prompt, **execute** `diskpart` to access the tool.

6. At the PowerShell prompt, **execute** `list vol` to list the volumes and partitions.

   In the list, identify the backup volume. In the next steps, you will select and format it.

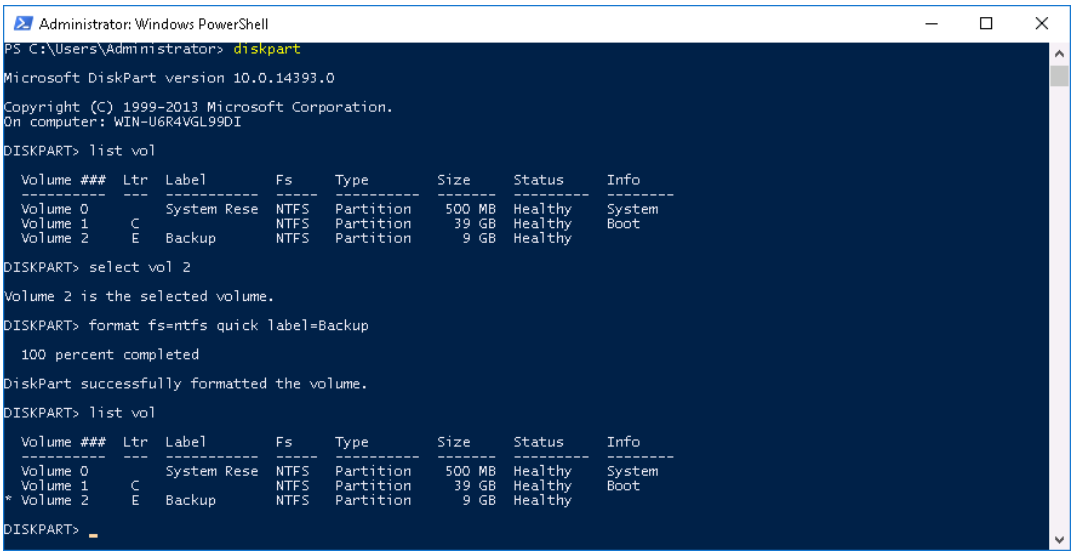


List volumes with diskpart

7. At the PowerShell prompt, **execute** `select vol 2` to select the backup volume.

8. At the PowerShell prompt, **execute** `format fs=ntfs quick label=Backup` to format the drive and assign a label to identify its use.

9. At the PowerShell prompt, **execute** `list vol` to verify the active volume.



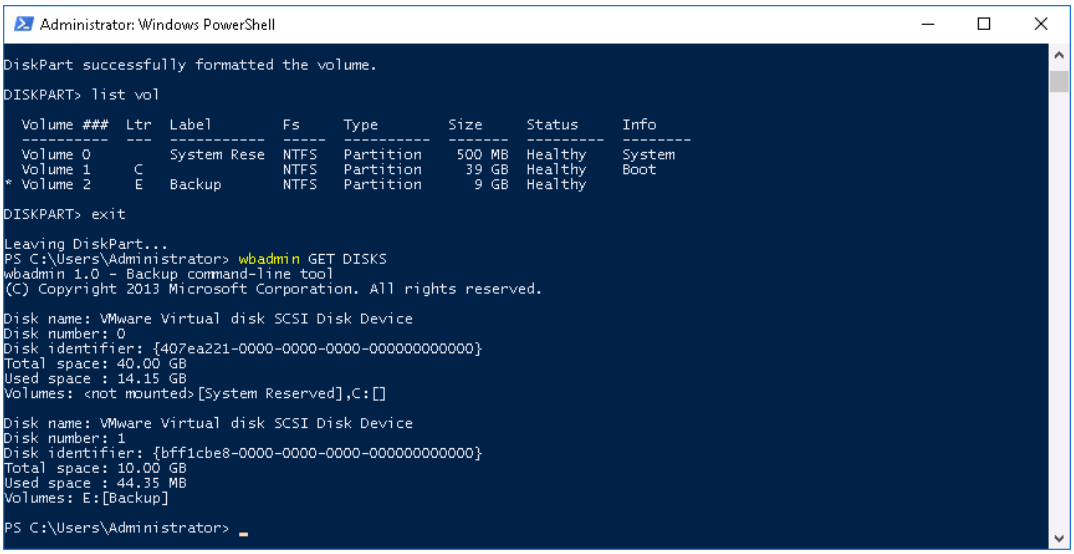
Verify volume

10. At the PowerShell prompt, **execute** **`exit`** to close the diskpart tool.

Part 2: Configure (System State) Backup

Note: In this part of the lab, you will use cmdlet commands to schedule a system state backup. First, you will need to identify the Disk that will be used as your dedicated backup drive.

1. At the PowerShell prompt, **execute** **`wbadmin GET DISKS`** to use the Web Server Backup's command line tool (wbadmin) to identify the backup disk.



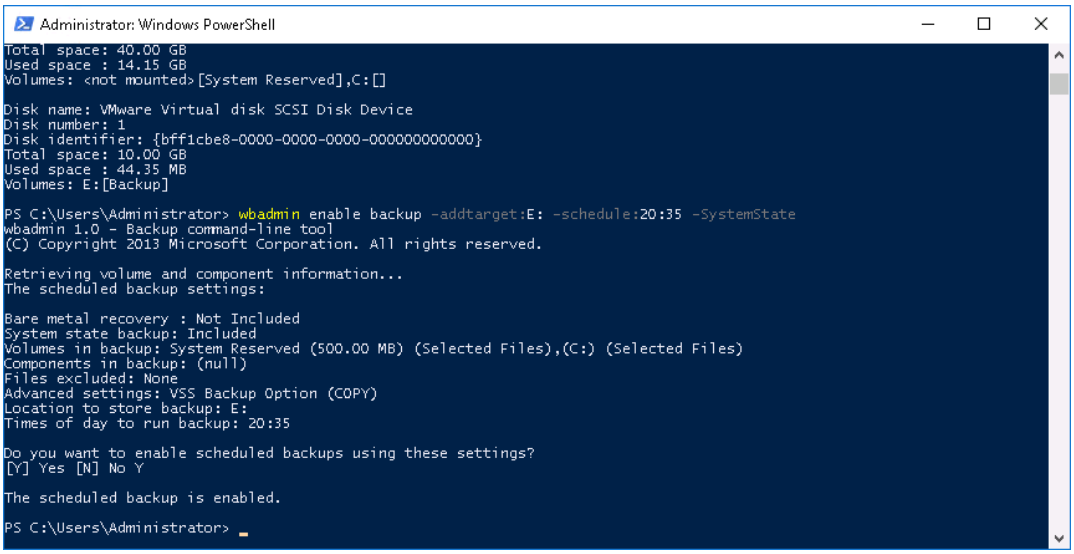
Identify backup disk

Note: In the next steps, you will use the E:[Backup] drive to create a daily schedule. Before you begin, identify the current time displayed on the TargetWindows01 machine in the lab. Scheduled events, such as a daily backup, use military time and depend on the system clock of the machine performing the action, in this case, performing a back up.

In the following step, replace the italicized time in the command with the system time on your lab session plus 5 minutes. For example: If your system time is 8:30PM, replace the time in the command with 20:35.

2. At the PowerShell prompt, **execute** `wbadmin enable backup -addtarget:E: -schedule:20:35 -SystemState` to set a schedule daily time for a system state backup.

3. When prompted, **execute** `Y` to create a scheduled backup to take place in 5 minutes.



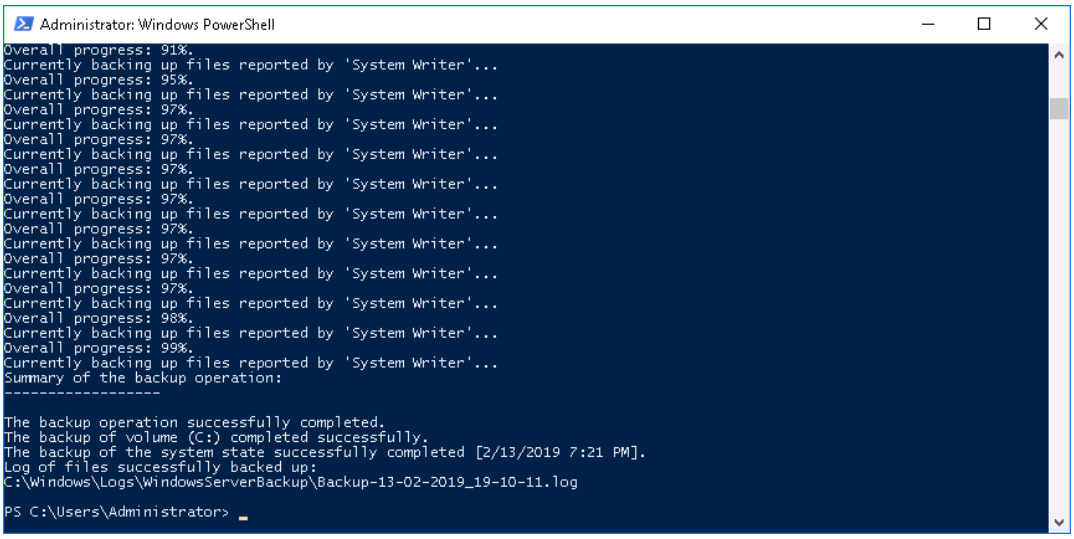
Schedule a System State backup

4. **Make a screen capture** showing the **scheduled backup settings** and **paste** it into your Lab Report file.

   You will have to wait the 5 minutes specified in the command before the backup process begins. The backup itself takes several minutes. You will be able to watch the progress in the next steps.

5. At the PowerShell prompt, **execute** `wbadmin get status` to watch the progress of the backup as it is running.

   This process takes several minutes. Once completed, the status will show the location of the log where the backup is stored.



Completed backup

6. At the Powershell prompt, **execute** `copy-item -path filepath -destination C:\Users\Administrator\Desktop`, replacing *filepath* with the log file's location, to copy the **log file** to the TargetWindows01 desktop.

7. **Close** the **PowerShell window** and **minimize** the **remote TargetWindows01 connection**.

Part 3: Configure Websites to use a Common NFS Share

Note: In this part of the lab, you will configure redundant web servers (www1 and www2) to use an NFS on a third storage server for web content. Originally used in the UNIX operating system, NFS is used to make remote folders appear as part of the local file system on Linux and even Windows systems.

1. On the vWorkstation taskbar, **click** the **Internet Explorer icon** to open the browser.

2. **Open** `http://www.securelabsondemand.com` to view the content of the master default web page.

3. **Open** `http://www1.securelabsondemand.com` to view the content of the default web page for that URL.

4. **Open** `http://www2.securelabsondemand.com` to view the content of the default web page for that URL.

   You will notice that the content of the default web page is different on each website. In the next steps, you will configure the www1 and www2 sites to become a redundant version of the master www website.

5. **Close** the **Internet Explorer**.

6. In the Connections folder, **open a PuTTY session** to **storage**.

7. At the command prompt, **execute** the **command** to change the current directory to **/etc**.

Note: In the next steps, you will use the Nano command line editor to modify files in the lab. The editor includes on screen prompts for basic commands such as save and quit; other commands can be found on the Internet.

8. At the command prompt, **execute** `nano exports` to open the exports file in the Nano editor.

9. After the last line of text in the file, **type** `/var/www *(rw,root_squash,sync,no_subtree_check,crossmnt)`.

10. **Press CTRL+X** to save your changes to the exports file; when prompted, **confirm** the changes and **save** the file as **exports**.

11. At the command prompt, **execute** `cat exports` to verify that the new line was added and saved correctly.

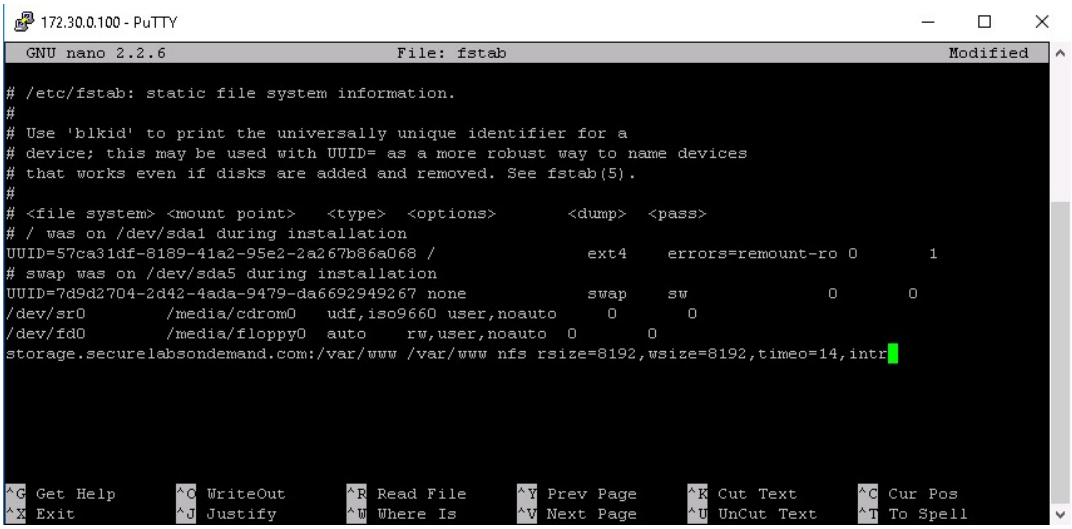
12. At the command prompt, **execute** `/etc/init.d/nfs-kernel-server restart` to restart the NFS server daemon, then **close** the **PuTTY session**.

13. In the Connections folder, **open a PuTTY session** to **www1**.

14. At the command prompt, **execute the commands** to open the **/etc/fstab** file in the Nano editor.

Note: The fstab file instructs Linux systems which mount points are available and how to access them, so they can be mounted automatically upon start up.

15. After the last line of text in the file, **type** `storage.securelabsondemand.com:/var/www /var/www nfs rsize=8192,wsize=8192,timeo=14,intr`.



Add a new line to the file

16. **Save** the changes to the fstab file.

17. At the command prompt, **execute** `mount -a` to mount the new point.

18. At the command prompt, **execute** `df -h` to check the mount point.

19. **Make a screen capture** showing the **www1 filesystem mount point** and **paste** it into your Lab Report file.

20. **Close** the **PuTTY session**.

21. **Repeat steps 12-19** for the www2 shortcut.

22. **Open** the **Internet Explorer** browser and **open http://www.securelabsondemand.com**, the master default web page.

23. In the browser, **open http://www1.securelabsondemand.com** to view the content of the default web page.

    You will see updated web content hosted on the common NFS mount (/var/www on storage). If you do not see new content, **refresh** the **browser page**.

24. **Repeat step 22** for the http://www2.securelabsondemand.com site.

25. **Close Internet Explorer**.

Part 4: Use Windows to Back Up the Common NFS Share

Note: In the next steps, you will configure TargetWindows01 to automatically back up the /var/www NFS share on the storage server. Using Windows 2016 Server's native Client for NFS commands, you will mount the NFS server called storage.

1. **Restore** the **TargetWindows01 connection** and **launch** a **Command Prompt window**.

Note: In the next steps, you will configure TargetWindows01 automatically back up the /var/www NFS share on the storage server. You will begin with the *mount* command. The command and the options used in the section are described below:

```
mount -o mtype=hard 172.30.0.200:/var/www *
```

- `mount` attaches the file system
- `-o` introduces a list of options
- `mtype` can be specified as hard or soft
  - (Hard: Will attempt to reconnect to the NFS without errors if the NFS becomes unavailable)
  - (Soft: Will attempt to reconnect to the NFS but will report an error if NFS is unavailable)
- `172.30.0.200:/var/www` is the IP address and path that will be shared
- `*` (the asterisk) is a wildcard that directs the command to use any available drive letter for the new share

2. At the command prompt, **execute** `mount -o mtype=hard 172.30.0.200:/var/www *` to mount /var/www on storage.securelabsondemand.com to the next available drive on TargetWindows01.

3. At the command prompt, **execute** `mklink /D c:\www z:` to create the share folder.

Note: The mklink command creates a symbolic link so that remote Z: drive can be accessed as local folder called www on the C: drive. This type of link enables tools like xcopy to work on remote drives by making them appear local to the OS.

4. **Make a screen capture** showing the **symbolic link for c:\www** and **paste** it into your Lab Report file.

5. At the command prompt, **execute** the **commands** to change the directory to **c:\www** and **list the contents**.

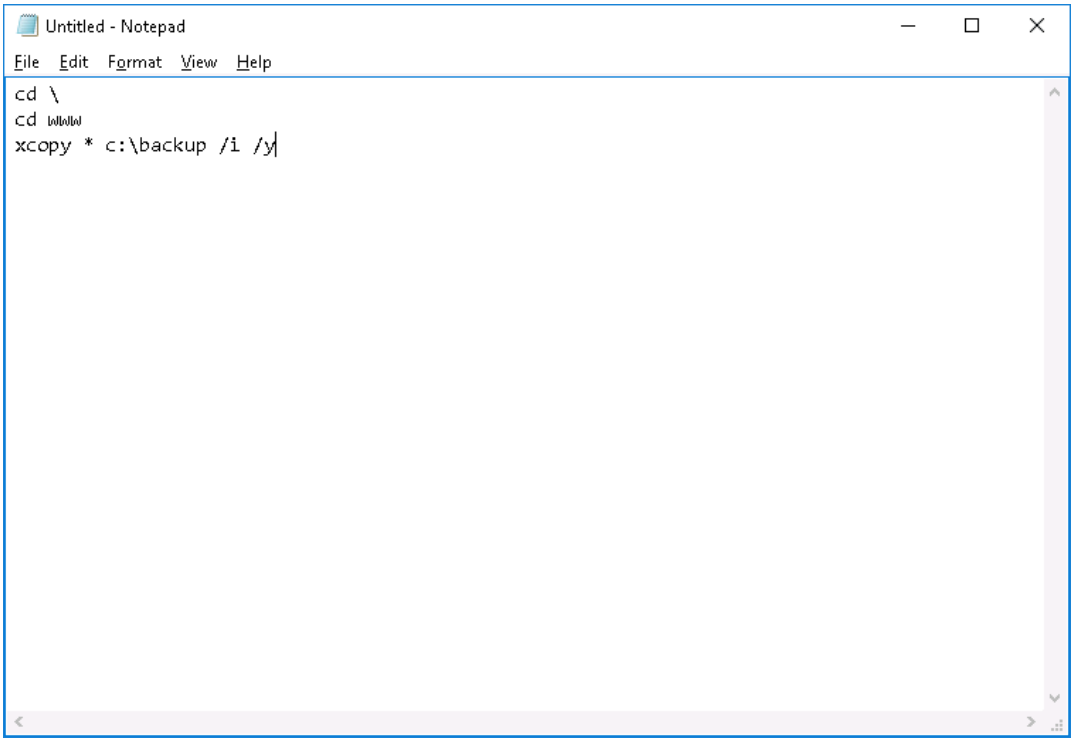
6. **Make a screen capture** showing the **contents of the c:\www directory** and **paste** it into your Lab Report file.

7. **Close** the **Command Prompt window**.

Note: In the next steps, you will create a batch file. A batch file is a text file containing a series of commands that the computer should execute. First, you will create the text file to use xcopy to create a backup copy of the new www folder (creating a new backup folder when necessary and overwriting existing files each time the command is run), and then you will schedule that backup command to recur every day.

8. On the TargetWindows01 desktop, **create a batch file** named ***yourname*_wwwbackup.bat**, replacing *yourname* with your own name, to back up the contents of c:\www to c:\Backup, as shown in the following figure.

   Because this is a batch file, it can be run on demand. In the next step, you will run the batch file to create a backup.



Create the batch file

9. From the TargetWindows01 desktop, **run *yourname*_wwwbackup.bat** to create a backup of the c:\www directory.

10. **Open** the **File Explorer** and **navigate** to **C:\backup** to verify that the Backup process copied the files from the www directory.

11. **Make a screen capture** showing the **contents of the C:\backup directory** and **paste** it into your Lab Report file.

Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

12. From the TargetWindows01 desktop, **select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

    - **Backup-*datetime*.log**
    - ***yourname*_wwwbackup.bat**

13. **Minimize** the **remote TargetWindows01 connection**.

14. On the vWorkstation desktop, **right-click** and **select Paste** to paste the copied files to the Desktop.

    If necessary, **close** the **Connection folder**.

15. On the vWorkstation desktop, **drag** the deliverable files into the File Transfer folder to complete the download to your local computer.

Section 3: Lab Challenge and Analysis

Note: The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

Part 1: Analysis and Discussion

In the lab, you installed the Client for NFS feature that enabled you to create a file share. Research the component, NFS, and NFS authentication methods.

Part 2: Tools and Commands

Edit the batch file that you created in the lab so that it includes subdirectories and copies only those files that have changed since the previous backup.

Part 3: Challenge Exercise

Create a new directory (*yourname*, replacing yourname with your own name) on the storage server, then create a new NFS share on the TargetWindows01 machine to that new directory, as you did in the lab.