Introduction

To support the Availability component of the CIA triad, any mature security program must include a business impact analysis (BIA). The purpose of this document is to preemptively determine the impact to an organization in the event that key processes and technology become unavailable. The BIA should also identify the assets required for the business to recover from an event and continue doing business. These assets are identified through the risk analysis and assessment process, which determines the probability of a risk (such as an earthquake or a power outage) to occur and the impact that it 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 creating a business continuity plan (BCP). As the name implies, a BCP outlines plans for continuing essential business functions after a major disruption that impacts the availability of critical systems. The BCP must clearly define responsibilities and support structures for continued operations, such as facilities, personnel, equipment, software, data files, vital records, and contractor and service provider relationships. It should also include requirements for acceptable minimum downtime for each system, as well as key assumptions, accountabilities, and how frequently the plan should be tested to ensure that all key personnel are aware of their responsibilities.

In addition to the BCP, organizations must also develop disaster recovery plans (DRP) as an output of their BIA. Where the BCP outlines plans for continuing business operations immediately after a major disruption, the DRP defines plans for resuming normal business operations. In the context of IT infrastructure availability, the DRP should document the procedures for returning a specific system or subsystem to production in the event of failure or compromise. The nature of the compromising event ultimately determines the recovery effort required. For example, to recover from a short-term power loss, system administrators may only need 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 need to develop multiple BCPs specific to the risks of different regions (including the possibilities of war and terrorism).

In this lab, you will configure backup and recovery functions that support business continuity, disaster recovery, and high availability. You will begin by installing the Windows Server Backup feature and configuring a daily System State backup. You will then review the steps involved in restoring a Domain Controller from an existing System State backup. In Section 2, you will configure two web servers to use a common Network File System (NFS) share and set up load balancing on a pfSense firewall-router.

Lab Overview

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

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

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

3. In the third part of the lab, you will restore the Windows server from a System State Backup.

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. You will configure a Network File System (NFS) share and set up load balancing for two redundant web servers.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and 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.

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. Restore a Domain Controller from a System State backup.

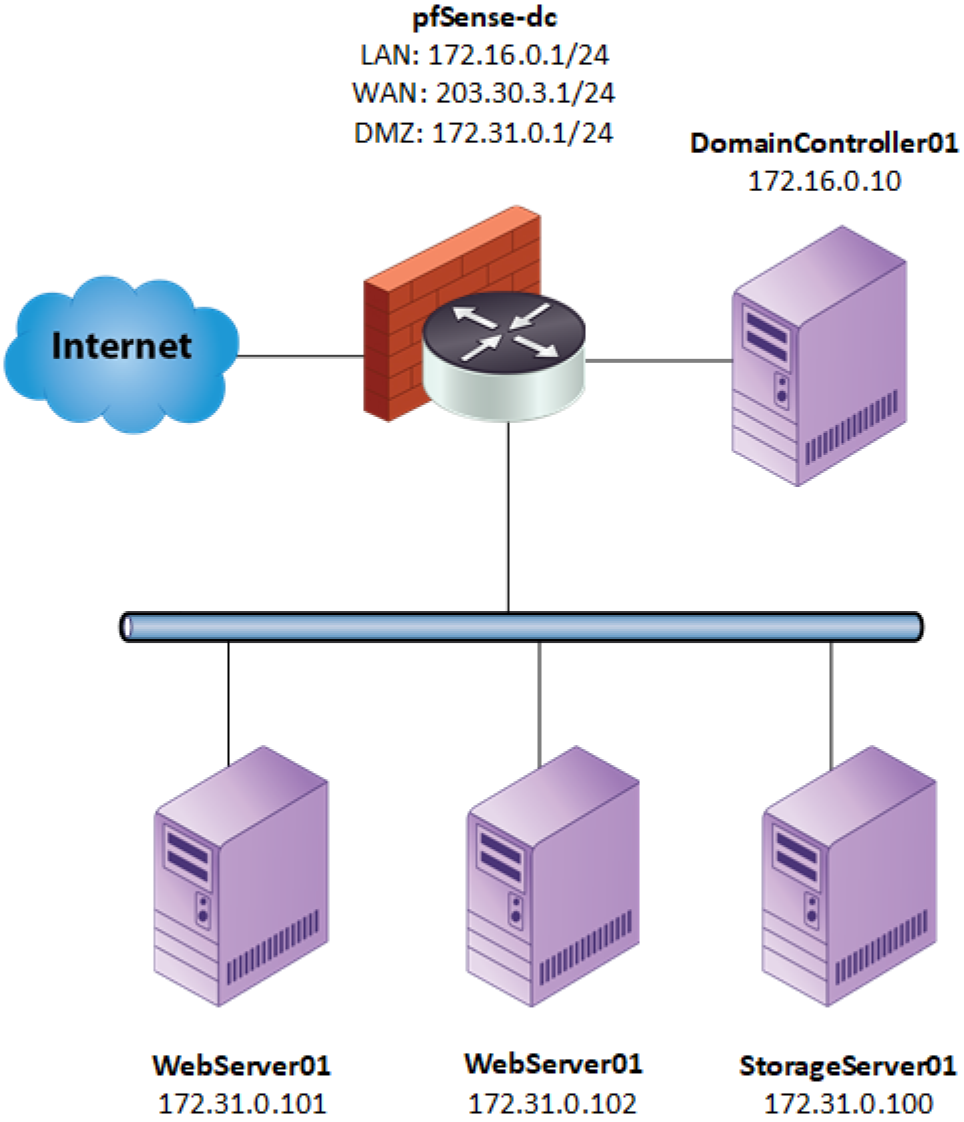
4. Configure a Linux NFS server and Linux NFS clients.

5. Configure load balancing across redundant web servers.

Topology

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

- DomainController01 (Windows: Server 2019)
- pfSense-dc (FreeBSD: pfSense)
- WebServer01 (Linux)
- WebServer02 (Linux)
- StorageServer01 (Linux)



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.

- Windows Server Backup
- Wbadmin
- NFS
- Vi Editor
- pfSense

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:

- Completed Windows Server Backup feature installation
- Scheduled Backup settings, including the destination and backup time
- Recovery Wizard Confirmation page

2. Any additional information as directed by the lab:

- None

SECTION 2

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

- Results of the reverse DNS query
- Updated webserver01 home page
- Updated webserver02 home page
- Http_server_pool backend
- Http_access frontend
- New Host Overrides entry for cscd.securelabsondemand.com
- Result of your DNS query for cscd.securelabsondemand.com
- Statistics Report with a value of at least 1 in the Sessions > Total column of the http_server_pool_ipvANY box, for both webserver01 and webserver02

2. Any additional information as directed by the lab:

- None

SECTION 3

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

- Updated Check Frequency value in the Health checking module
- HAProxy Statistics Report with a host in a DOWN state, as well as the UP host having more total sessions (http_server_pool_ipvANY, Sessions > Total) than the DOWN host

2. Any additional information as directed by the lab:

- None

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 deliverables.

1. **Review** the **Tutorial**.

   Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

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

Part 1: Install Windows Server Backup

Note: When selecting a Backup and Recovery solution, you must consider both business and technical requirements. Business requirements include key metrics like Recovery Time Objective (how much time should it take to restore this service?), Recovery Point Objective (how much data must be recovered?), and Mean Tolerable Period of Disruption (how long can the organization tolerate a disruption to this service?). Technical requirements include considerations such as vendor and product diversity (is the IT infrastructure predominantly Windows-based or Linux-based?), the degree of virtualization, and the number of systems to be backed up. This information should be documented during risk analysis as part of an IT Asset Inventory, which should identify, classify, and prioritize all of the systems within an IT infrastructure.

For businesses that use Microsoft products for enterprise management, Microsoft provides a variety of backup and recovery solutions at the PC, server, and enterprise levels:

- Windows File History for PCs – This automatically backs up files and specified directories on a PC’s local data stores on an incremental basis, allowing specific revisions to be restored using the “History” function in the Windows File Explorer.

- Windows Server Backup for servers – This allows you to schedule backups of specified files, directories, or drives, and it allows you to designate a backup location, which can be located on a network drive.

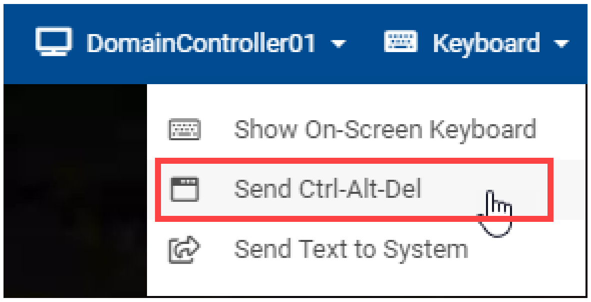
- Data Protection Manager – This backs up applications, files and directories, systems, and virtual machines to disks, Azure, or tape. It can be used for near-continuous protection, optional tape-drive backups, and can restore data to an alternate location.

- Microsoft Azure Backup Server (MABS) – This backs up large-scale virtual or hybrid deployments to the Microsoft Azure cloud; it incorporates other backup and recovery solutions. You can read more about MABS here.

In this part of the lab, you will install the Windows Server Backup on a Windows 2019 Server using the Server Manager. Windows Server Manager provides a console for administrators to execute backups on local (or on-premise) and remote (or offsite) servers.

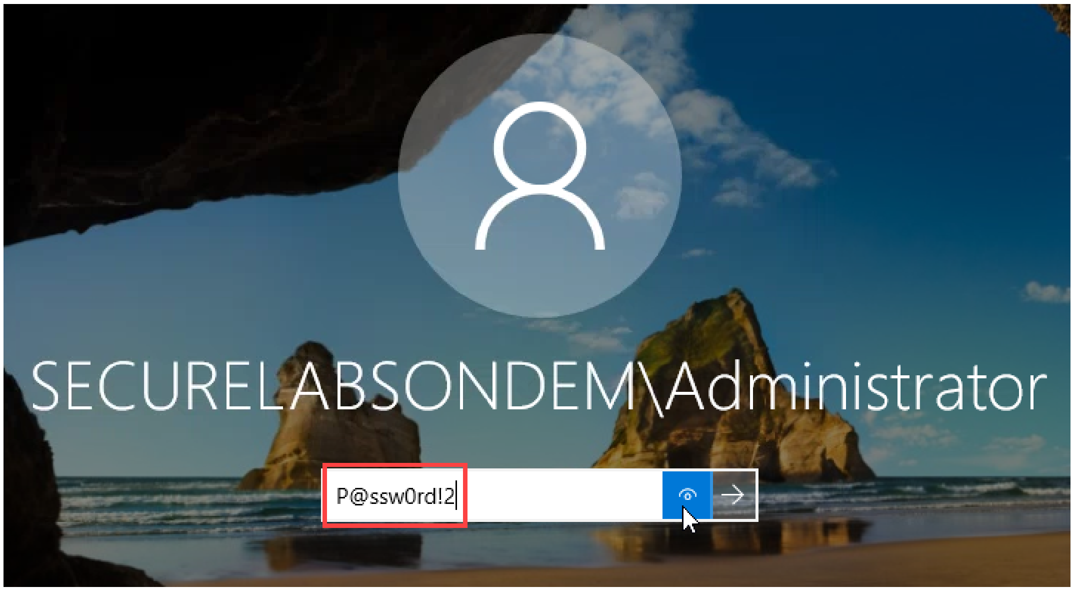
In the next steps, you will open the Server Manager and launch the Add Roles and Features Wizard.

1. On the Lab View toolbar, **select Keyboard > Send Ctrl-Alt-Delete** to send the Ctrl-Alt-Delete command to the DomainController01 system.



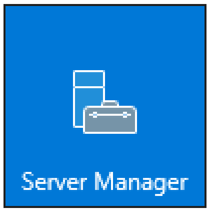
Keyboard menu

2. At the log-in prompt, **type** **`P@ssw0rd!2`** and **press Enter** to log in as the domain administrator.



Log-in prompt

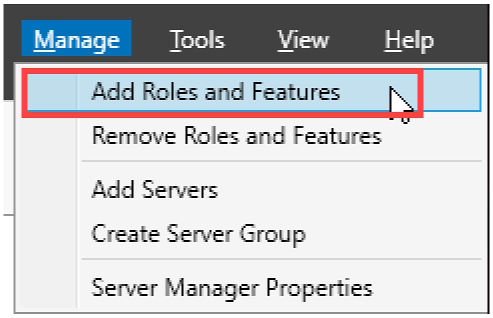
3. On the DomainController01 taskbar, **click** the **Windows Start icon**, then **click** the **Server Manager button** to open the Server Manager application.



Server Manager button

Note: You should see Welcome to Server Manager with 5 options and Roles and Server Groups. It currently shows 3 roles (AD DS, *Active Directory Domain Services*; DNS, *Domain Name Service*; File and Storage Services) and 1 server group (Local Server). Server groups allow you to manage multiple servers at once, which can facilitate recovery plans. The roles define the functions a server takes on within a network. The AD DS role manages storage of information about user accounts, enables authorized users to access information, and much more. The DNS role maps host names to IP addresses within a domain. The File and Storage Services role manages file storage and sharing within a network/domain.

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



Manage > Add Roles and Features

Note: The Windows Server Backup is a new feature that will be added, so it uses the Role-based or feature-based installation. There is also only one machine available to choose for installation.

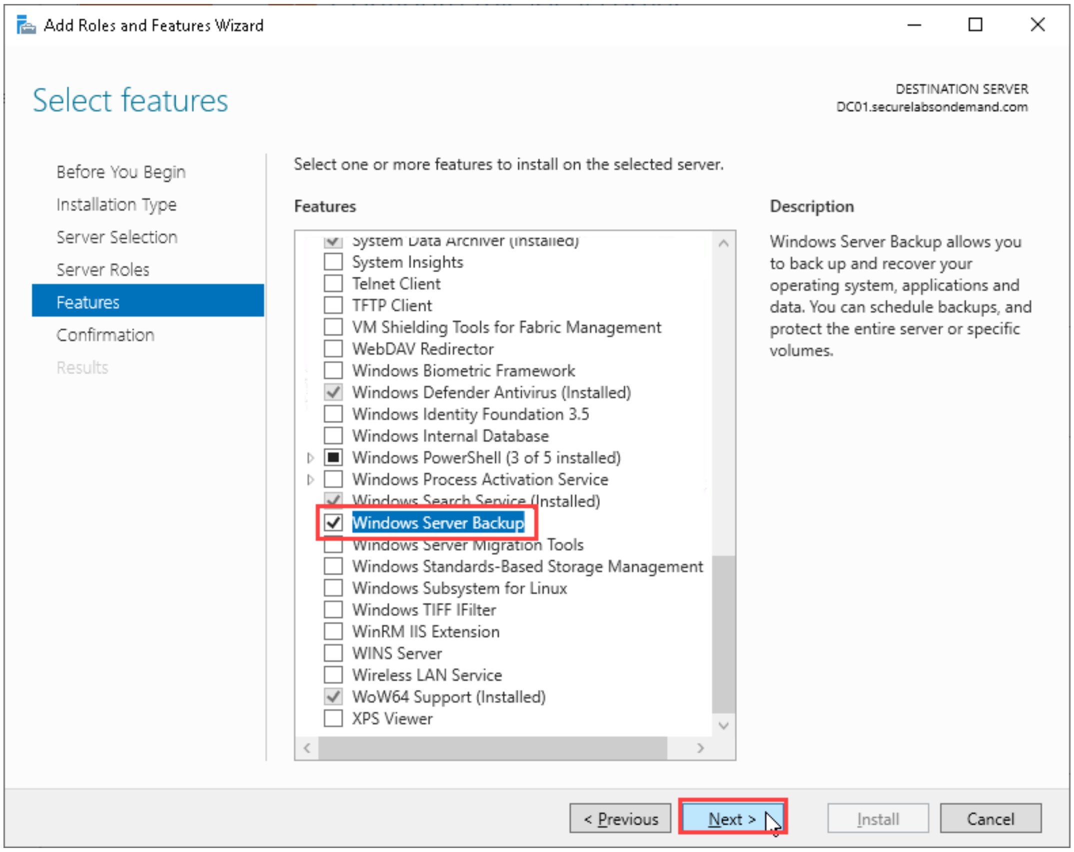
5. On the Before You Begin page, **click Next** to continue.

6. On the Installation Type page, **click Next** to accept the default (Role-based or feature-based installation) and continue.

7. On the Server Selection page, **click Next** to accept the default selection (DC01, the DomainController01 server) and continue.

8. On the Server Roles page, **click Next** to continue.

9. On the Features page, **click** the **Windows Server Backup checkbox**, then **click Next** to continue.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
DC01.securelabsondemand.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- ☑ System Data Archiver (Installed)
- □ System Insights
- □ Telnet Client
- □ TFTP Client
- □ VM Shielding Tools for Fabric Management
- □ WebDAV Redirector
- □ Windows Biometric Framework
- ☑ Windows Defender Antivirus (Installed)
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ▷ ■ Windows PowerShell (3 of 5 installed)
- ▷ □ Windows Process Activation Service
- ☑ Windows Search Service (Installed)
- ☑ Windows Server Backup
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management
- □ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- □ WinRM IIS Extension
- □ WINS Server
- □ Wireless LAN Service
- ☑ WoW64 Support (Installed)
- □ XPS Viewer

Description

Windows Server Backup allows you to back up and recover your operating system, applications and data. You can schedule backups, and protect the entire server or specific volumes.

Features page

10. On the Confirmation page, **click Install** to install the selected feature.

11. **Make a screen capture** showing the **completed Windows Server Backup feature installation**.

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

Part 2: Configure a System State Backup

Note: In this part of the lab, you will use Windows Server Backup to make a daily System State backup for the DomainController01 server. Backups are generally divided into two types:

- File backups - these generally refer to personal files stored on a device, such as photos and documents stored in the user directories.

- System State backups - these refer to the current operating system state and configuration, which accounts also for system files, application data, and entries in the Windows registry, with the aim of returning your machine back to the same state it was in when the snapshot was taken.

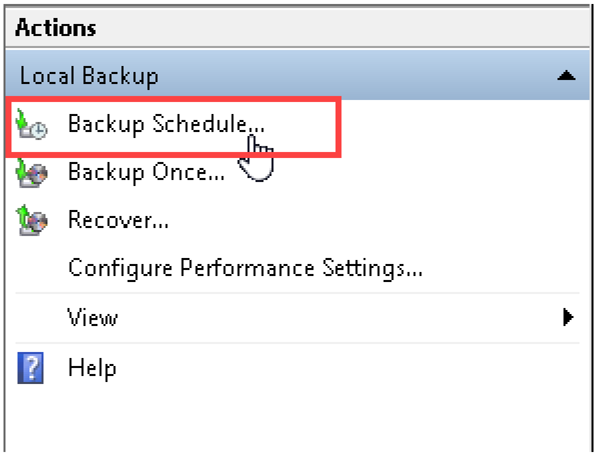
A system state backup includes domain controller functions and Active Directory services, and can be recovered onto a different server, which can minimize downtime during disaster recovery.

In the next steps, you will open the Windows Backup Admin console and begin the process of scheduling your daily backup.

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

Note: This may take a minute to load. You should see an amber caution sign in the center pane indicating that a scheduled backup has not been configured for this computer. In the next steps, you will launch the Backup Schedule wizard and configure a scheduled backup of the local system.

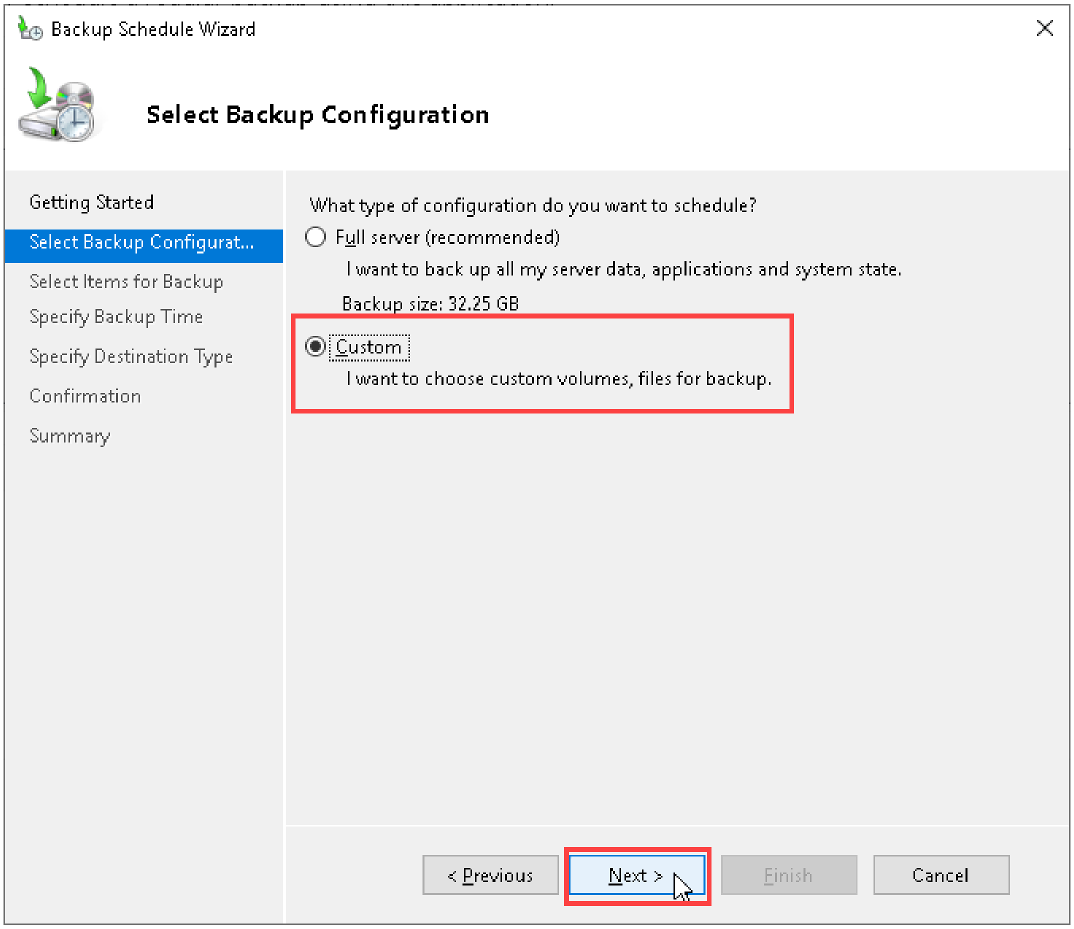
2. In the right pane of the wbadmin, **click Backup Schedule...** to launch the Backup Schedule wizard.



Backup Schedule

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

4. On the Select Backup Configuration page, **click** the **Custom radio button**, then **click Next** to continue.



What type of configuration do you want to schedule?

○ Full server (recommended)

I want to back up all my server data, applications and system state.

Backup size: 32.25 GB

● Custom

I want to choose custom volumes, files for backup.

Select Backup Configuration page

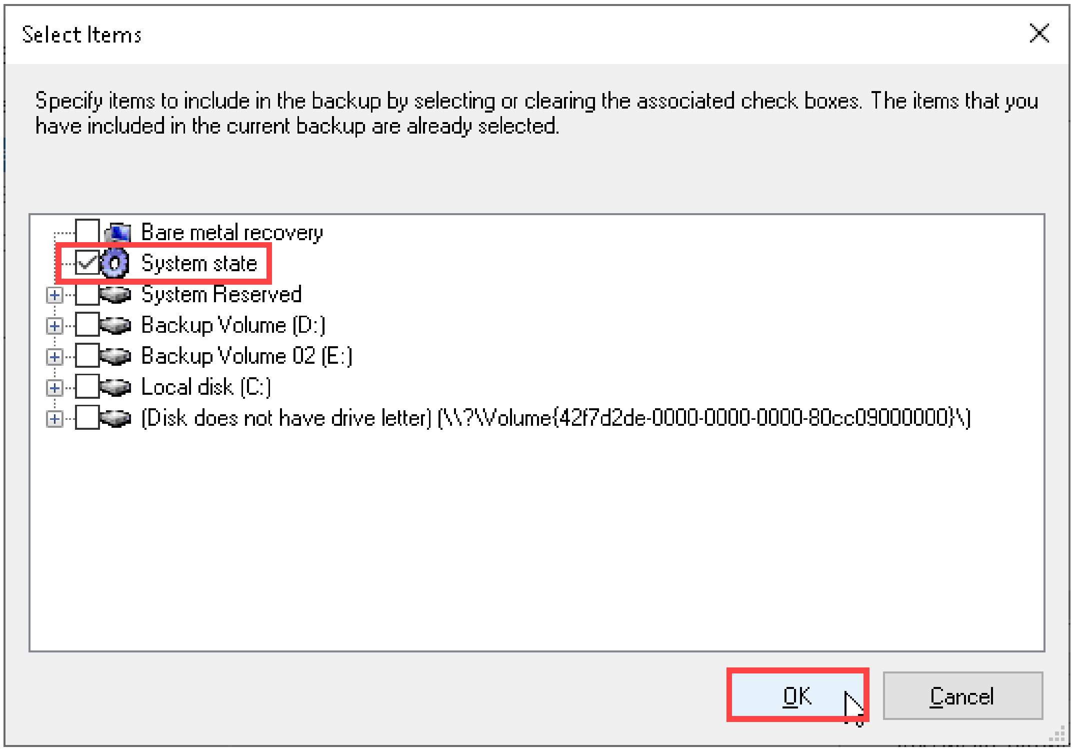
Note: Recall the two backup models that were discussed earlier – File and System State. The Full server option represents a combination of both options, and backs up server data as well as application data and the state of the system. The Custom option allows you to specify which model your scheduled backup will use and select individual files, folders, and disks.

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

Note: You will include only the *System state* item in this backup. Other options include:

- Bare metal recovery backs up operating system files, including the registry.
- System Reserved backs up the Boot Manager and Boot Configuration Data as well as startup files.
- Backup Volume (D:), Backup Volume 02 (E:), Local disk (C:), (Disk does not have a drive letter) (\\?\Volume(4217d2de...\) backs up the specified drives or drive partitions.

6. In the Select Items dialog box, **click** the **System state checkbox** to select the System State for backup, then **click OK** to close the dialog box.



Select Items

Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

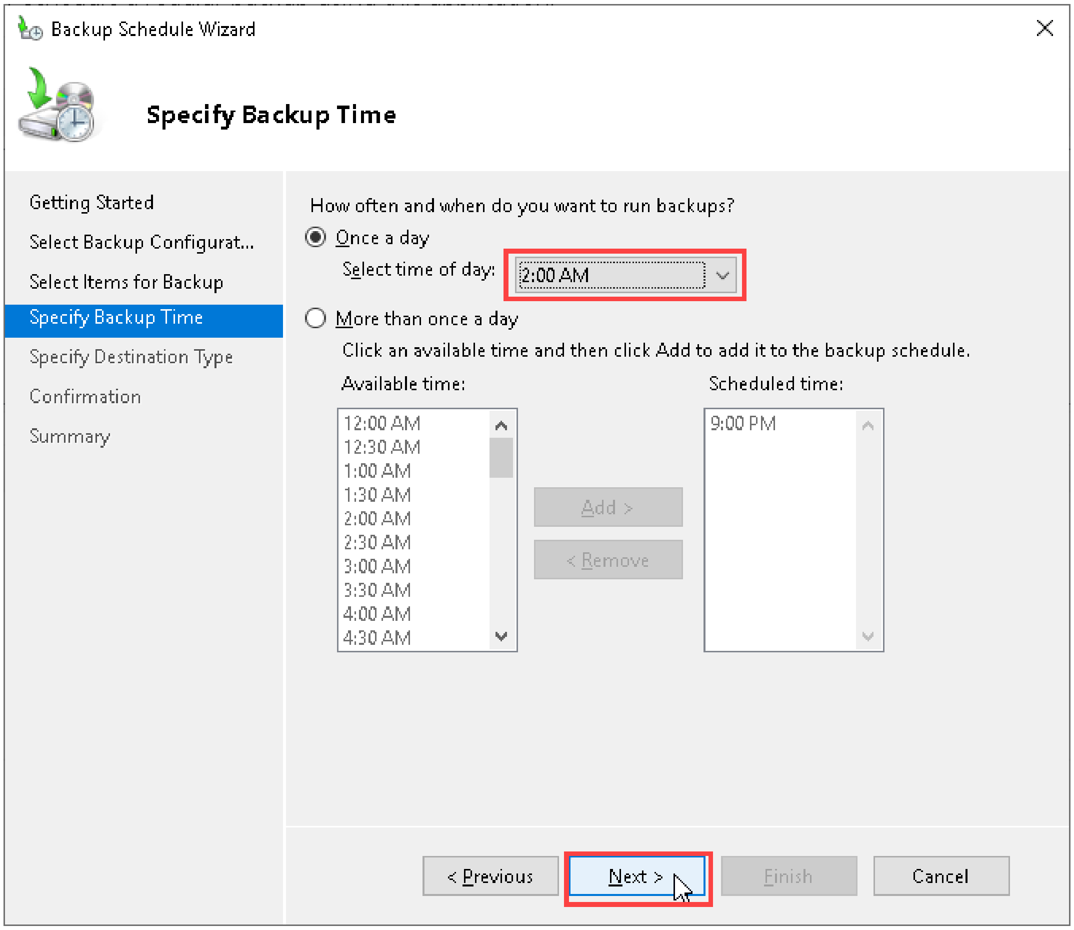
□ Bare metal recovery
☑ System state
□ System Reserved
□ Backup Volume (D:)
□ Backup Volume 02 (E:)
□ Local disk (C:)
□ (Disk does not have drive letter) (\\?\Volume{42f7d2de-0000-0000-0000-80cc09000000}\)

Select Items dialog box

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

Note: In the next step, you will set a specific time for when your system state backup will occur. Scheduling regular backups contributes to continued availability in the event of disruption or disaster. The frequency of backups should be defined in your BCP and DRP. It is also good to schedule backups for times when the server load will be low.

8. On the Specify Backup Time page, **select 2:00 AM** from the Time of Day menu, then **click Next** to continue.



How often and when do you want to run backups?

● Once a day

Select time of day: 2:00 AM

○ More than once a day

Click an available time and then click Add to add it to the backup schedule.

Available time: 12:00 AM, 12:30 AM, 1:00 AM, 1:30 AM, 2:00 AM, 2:30 AM, 3:00 AM, 3:30 AM, 4:00 AM, 4:30 AM

Scheduled time: 9:00 PM

Set time of day for backup

Note: You should now see the following options:

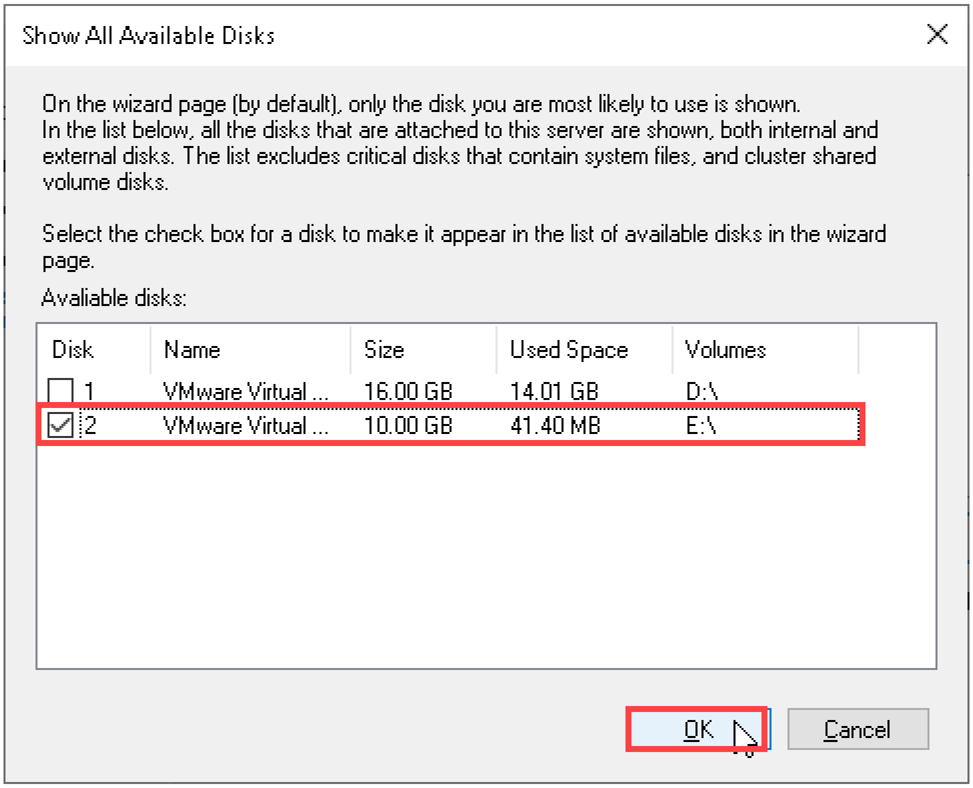
- Back up to a hard disk that is dedicated for backups (recommended) – This hard disk will be formatted, so it will only be used for backups.
- Back up to a volume and Back up to a shared network folder – These options back up to any volume/partition on a hard drive or shared network folder, which means that their resources can also be used for non-backup purposes.

The backup destination you select should have ample storage space, and its location should serve your BCP and DRP. To optimize availability, the backup should be located on a different site than the server that is being backed up. In the next step, you will set the destination type for your scheduled backup.

9. On the Specify Destination Type page, **click Next** to accept the default option (Back up to a hard drive that is dedicated for backups) and continue.

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

11. 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.



Show All Available Disks

On the wizard page (by default), only the disk you are most likely to use is shown.
In the list below, all the disks that are attached to this server are shown, both internal and external disks. The list excludes critical disks that contain system files, and cluster shared volume disks.

Select the check box for a disk to make it appear in the list of available disks in the wizard page.

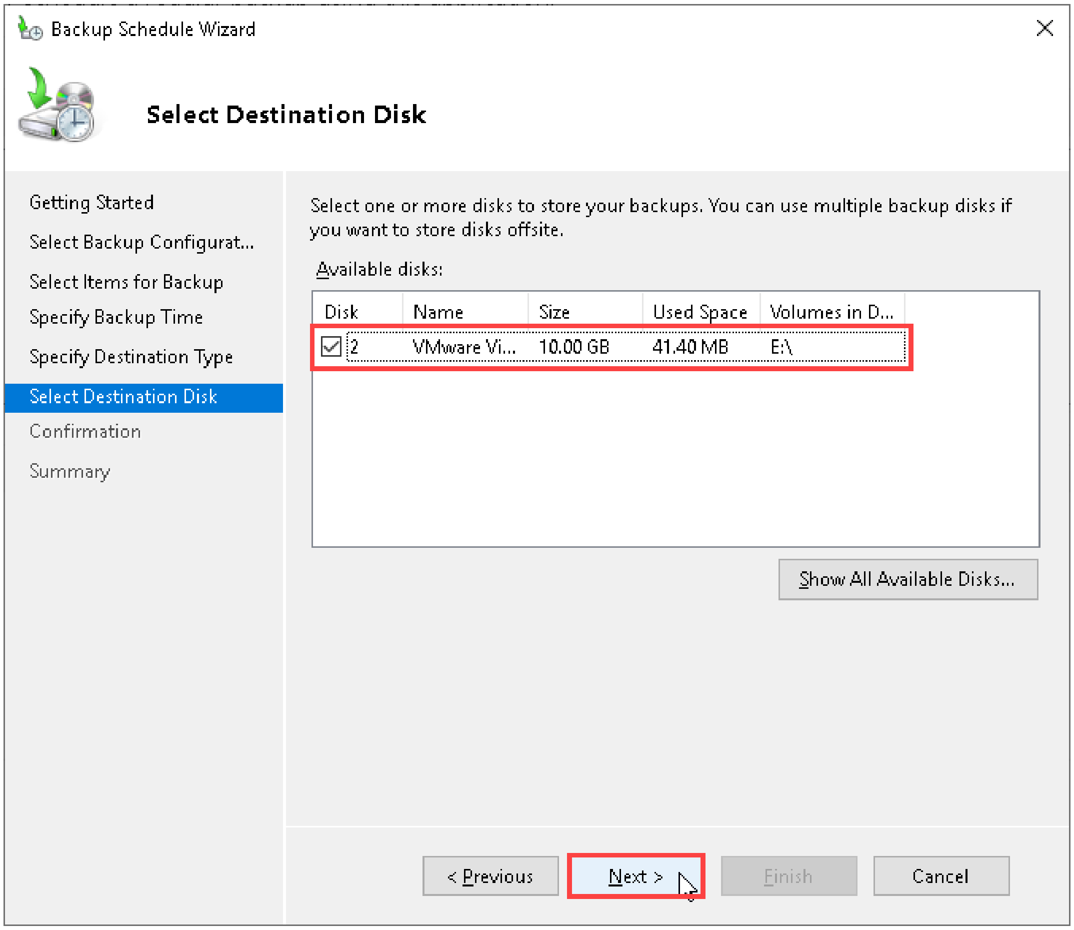
Avaliable disks:

Disk	Name	Size	Used Space	Volumes
□ 1	VMware Virtual ...	16.00 GB	14.01 GB	D:\
☑ 2	VMware Virtual ...	10.00 GB	41.40 MB	E:\

Show All Available Disks dialog box

Note: This is the file system and directory on which you will back up files. If your drive is too small to accommodate the backup, Windows will force the drive offline, making it unusable**.**

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



Select Destination Disk

Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.

Available disks:

Disk	Name	Size	Used Space	Volumes in D...
☑ 2	VMware Vi...	10.00 GB	41.40 MB	E:\

Select Destination Disk page

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

13. When prompted, **click Yes** to close the confirmation dialog box, then **click Finish** to continue.

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

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

Note: The wbadmin window will display the next scheduled backup time and information about the backup destination in the center pane. It will also display the status and time of the most recent backup, a list of All Backups, and messages from backup activity within the past week.

15. **Make a screen capture** showing the **Scheduled Backup settings, including the destination and backup time**.

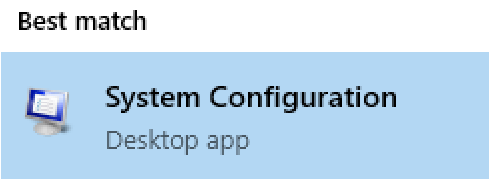
16. **Close** any **open windows**.

Part 3: Restore from a System State Backup

Note: In this part of the lab, you will walk through the process of restoring the DomainController01 server from an existing System State backup. System State recovery will return a system (or install a new server) to its pre-failure state without needing to reconfigure Windows. This can minimize downtime (or MTTR – mean time to repair/restore) in the event of a failed drive or disaster. As such, regular system state backups of an organization's critical endpoints (like their domain controllers) are likely to be prescribed within a BCP or DRP, which will ultimately direct your recovery actions when a system becomes unavailable.

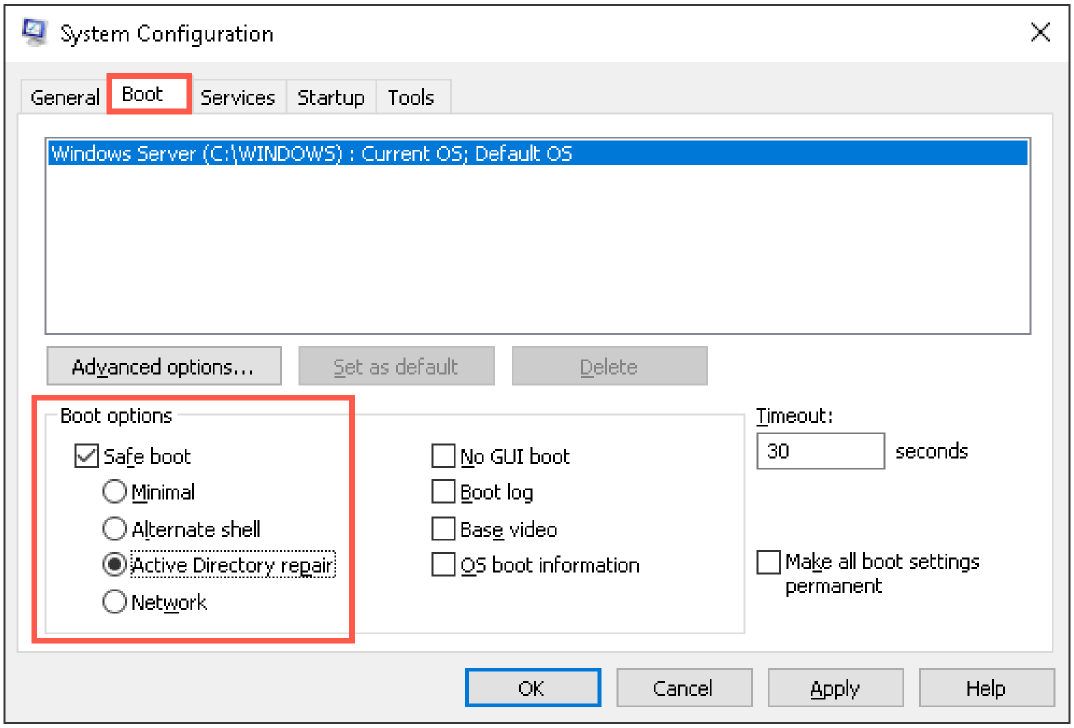
In the next steps, you will open the System Configuration application and configure the DomainController01 server to run in safe boot mode.

1. On the DomainController01 taskbar, **type** `System Configuration` in the Search bar, then **select** the **System Configuration desktop app** from the results.



System Configuration

2. In the System Configuration window, **click** the **Boot tab**, then **click** the **Safe boot checkbox** and **select** the **Active Directory repair radio button**.



Windows Server (C:\WINDOWS) : Current OS; Default OS

Boot options

☑ Safe boot

○ Minimal

○ Alternate shell

● Active Directory repair

○ Network

□ No GUI boot

□ Boot log

□ Base video

□ OS boot information

Timeout: 30 seconds

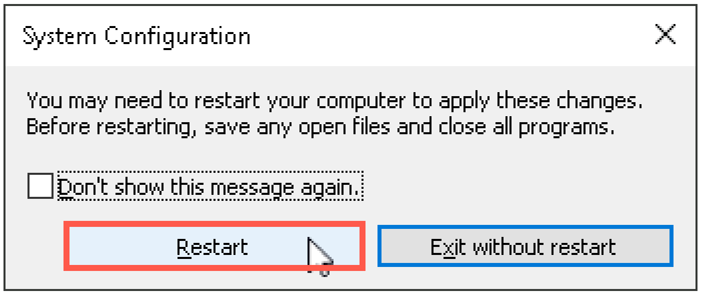
□ Make all boot settings permanent

Boot options

Note: Selecting these options ensures that the domain controller will boot into Directory Services Restore Mode (DSRM), which takes the Active Directory server offline. Windows does not allow you to restore an Active Directory that is online.

3. **Click OK** to apply your changes and close the System Configuration app.

4. When prompted, **click** the **Restart button** to restart the server.



System Configuration

You may need to restart your computer to apply these changes.
Before restarting, save any open files and close all programs.

□ Don't show this message again.

Restart the server

Note: The server will take a few minutes to restart. When the process is complete, you will see the Windows splash screen and a prompt to press Ctrl+Alt+Delete.

5. On the Lab View toolbar, **click Keyboard** and **select Send Ctrl-Alt-Del** to display the DomainController01 login prompt

Note: You have just booted your system into Safe Mode with DSRM. This mode ensures that Active Directory doesn't start, so the Domain Controller is not available, and you will need to log in to the local system instead of the Secure Labs On Demand domain.

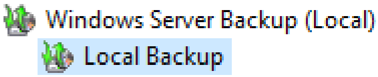
6. At the login prompt, **select Other user**, then **type** the following credentials and **press Enter** to log in as the local administrator.

   Username: **`.\Administrator`**
   Password: **`P@ssw0rd!2`**

Note: The Server Manager application will launch automatically upon login. You should see the Server Manager dashboard. In the Roles and Server Groups pane, all roles and server groups except File and Storage Services will display red title bars, indicating that they are currently unavailable.

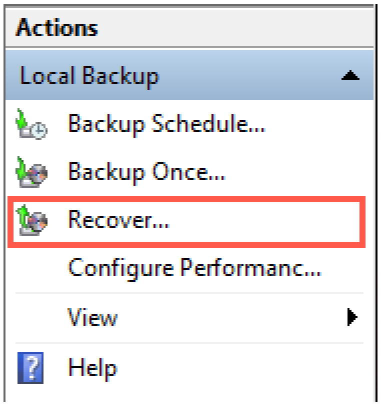
7. From the Server Manager menu bar, **select Tools > Windows Server Backup** to open the Windows Backup Admin (wbadmin) console.

8. In the left pane of the wbadmin console, **click Local Backup** to display the local backup options.



Local Backup

9. In the right pane of the wbadmin console, **click Recover** to launch the Recovery wizard.



Actions pane

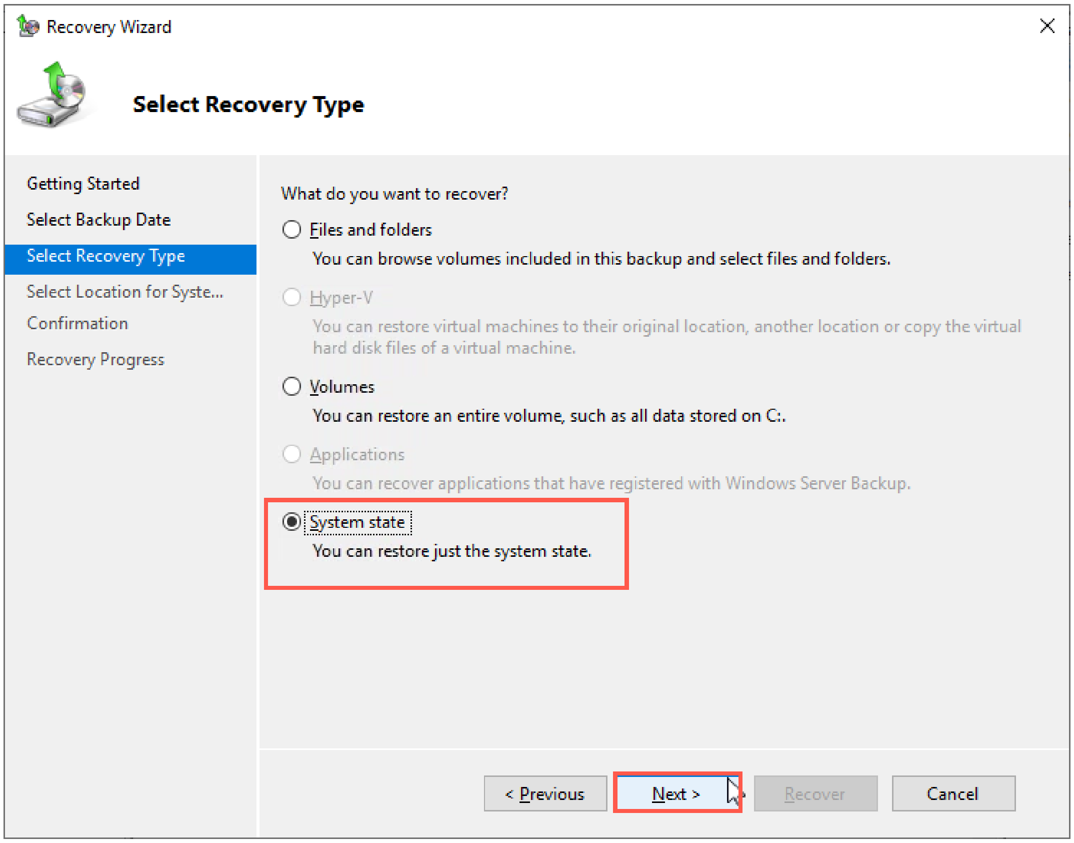
10. On the Getting Started page, **click Next** to accept the default selection (This server, DC01) and continue.

Note: Selecting this option informs the Recovery Wizard that your target backup file is stored locally on the DomainController01 server. This is sufficient for the purposes of this lab. However, best practices in production environments would ensure that the BCP and DRP direct you to back up files to a different physical location.

11. On the Select Backup Date page, **click Next** to accept the default selection (the backup dated 12/20/21 at 9:42 AM) and continue.

Note: For the purposes of this lab, you will use a pre existing backup of the System state stored on the DomainController01 server's D: drive.

12. On the Select Recovery Type page, **click** the **System state radio button**, then **click Next** to continue.



Recovery Wizard

Select Recovery Type

What do you want to recover?

○ Files and folders
You can browse volumes included in this backup and select files and folders.

○ Hyper-V
You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.

○ Volumes
You can restore an entire volume, such as all data stored on C:.

○ Applications
You can recover applications that have registered with Windows Server Backup.

● System state
You can restore just the system state.

Select Recovery Type

13. On the Select Location for System State Recovery page, **click Next** to accept the default selection (Original location) and continue.

14. At the Windows Server Backup dialog box, **click OK** to continue.

Note: For the purposes of this lab, you will stop here without actually running the restore, as this process would take more than an hour to complete.

15. **Make a screen capture** showing the **Recovery Wizard Confirmation page**.

16. **Click** the **Cancel button** to abort the system restore.

17. **Close** any **open windows**.

Note: This concludes Section 1 of the lab. If you have been assigned Section 2, you will need to reset your lab environment before beginning Section 2 (Options > Reset Lab).

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. You will configure a Network File System (NFS) share and set up load balancing for two redundant web servers.

Part 1: Configure an NFS Share

Note: In this section of the lab, you will take on the role of a network systems administrator who has been asked to convert a single-point-of-failure web server into a distributed system of web servers. To do this, you will separate data storage from the web servers' data transport services. You will set up a data storage server to use a Network File System (NFS). 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. This separation of functionality will allow you to scale the number of web servers available to end users as their demand commands.
In this part of the lab, you will configure two redundant web servers (webserver01 and werbserver02) to use NFS on a third storage server for web content. Redundancy in web servers means that each physical web server will use the same hard drive—in this case located on a storage server. Website requests will be routed by a firewall in order to ensure that collisions do not affect data accuracy for the users. Web server redundancy serves as de facto recovery in production environments, as the unavailability of one web server would not be noticed at the user level.

If you are continuing the lab from Section 1, ensure you have reset the lab environment (Options > Reset Lab).

1. On the Lab View toolbar, **select Keyboard > Send Ctrl-Alt-Delete** to send the Ctrl-Alt-Delete command to the DomainController01 system.

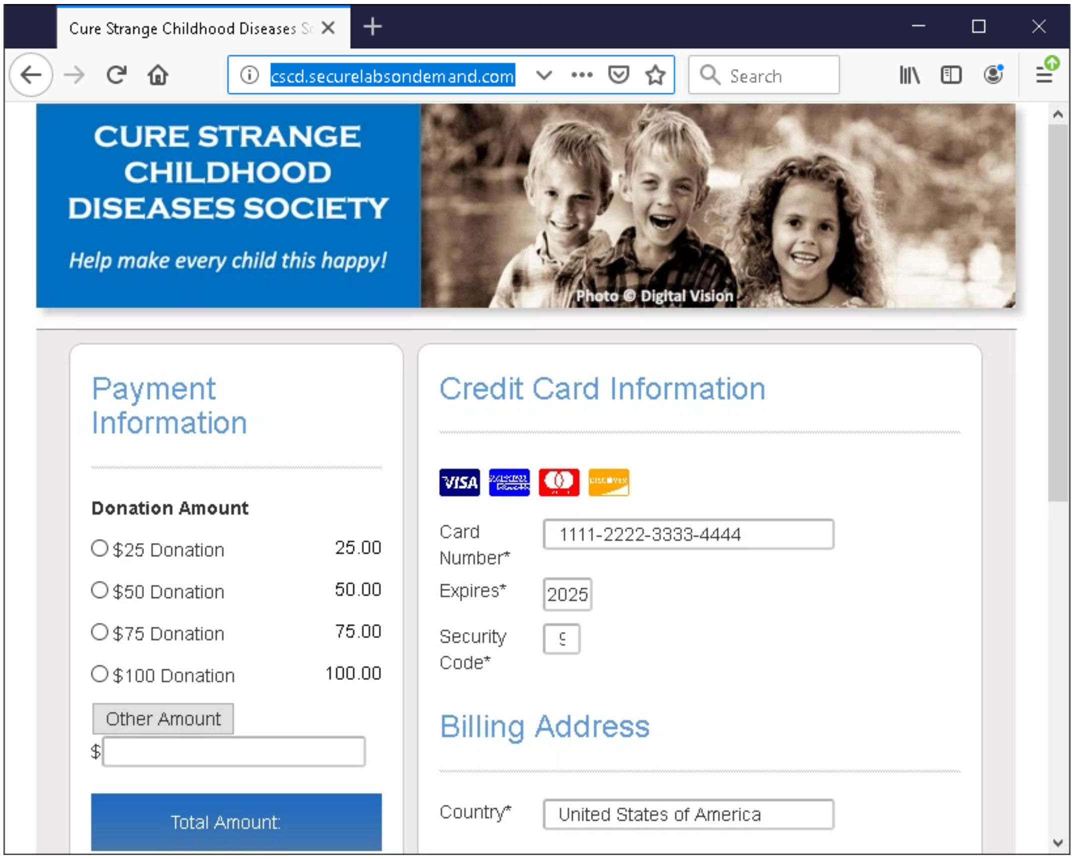
2. At the login prompt, **type `P@ssw0rd!2`** and **press Enter** to log in as the domain administrator.

3. On the DomainController01 taskbar, **click** the **Firefox icon** to open a new Firefox window.

Note: Robust information systems security practices require that domain controllers be housed on dedicated servers with limited functionality in order to minimize their attack surfaces. A critical service like your domain controller should have only software and services installed or running that pertain to its dedicated function. Unnecessary functionality only serves to broaden the attack surface and limit the performance of such a resource.

4. **Navigate** to `http://cscd.securelabsondemand.com` to view the content of the master default web page.

   If the website does not load on the first try, wait 30 seconds and try again.



Cure Strange Childhood Diseases S
cscd.securelabsondemand.com
Search

CURE STRANGE CHILDHOOD DISEASES SOCIETY

Help make every child this happy!

Photo © Digital Vision

Payment Information

Donation Amount

○ $25 Donation	25.00
○ $50 Donation	50.00
○ $75 Donation	75.00
○ $100 Donation	100.00

Other Amount

$

Total Amount:

Credit Card Information

Card Number* 1111-2222-3333-4444

Expires* 2025

Security Code* 9

Billing Address

Country* United States of America

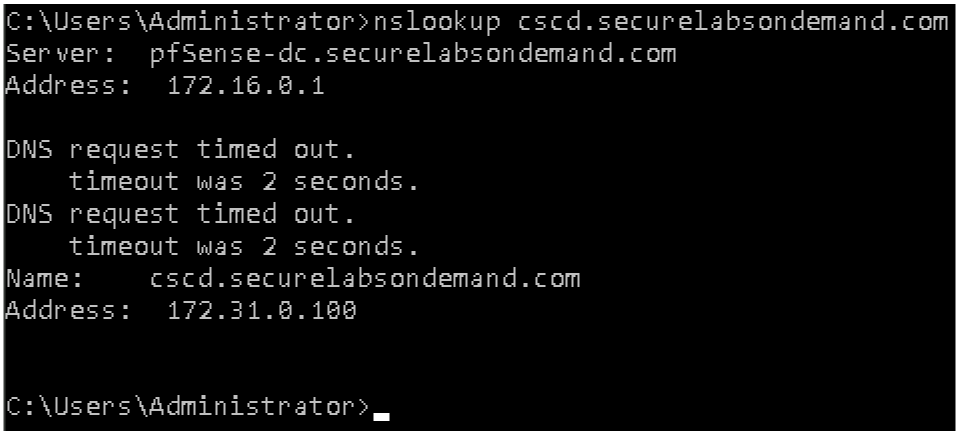
Cure Strange Childhood Diseases

Note: The CSCD Society website is currently being served by a single server on the DMZ network, which is actually recorded as storageserver01.securelabsondemand.com on the organization’s internal DNS server (also running on the domain controller). You intend to remove this server’s web serving responsibilities and convert it in into a dedicated NFS server. Later, you will be able to mirror this content to dedicated web servers to run several instances of your site in parallel.

In the next steps, you will review the current DNS configuration and identify which hostnames are associated with which IP addresses.

5. From the DomainController01 taskbar, **open** a **Command Prompt window**.

6. At the command prompt, **execute** `nslookup cscd.securelabsondemand.com` to perform a DNS lookup for cscd.securelabsondemand.com.



```
C:\Users\Administrator>nslookup cscd.securelabsondemand.com
Server:  pfSense-dc.securelabsondemand.com
Address:  172.16.0.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Name:    cscd.securelabsondemand.com
Address:  172.31.0.100


C:\Users\Administrator>
```

DNS lookup

Note: You should notice that this DNS record is provided by the pfsense-dc.securelabsondemand.com device, the perimeter firewall of this organization. In this scenario, it is also acting as the authoritative name server for the CSCD public website. In a real production environment, these functions are typically outsourced as part of site hosting or domain name packages, or run through cloud service providers, which may offer high-availability features such as DDoS protection.

In the next step, you perform a reverse DNS lookup, this time specifying the internal domain controller as the DNS server.

7. At the command prompt, **execute** `nslookup 172.31.0.100 172.16.0.10` to perform a reverse DNS query on the IP address for cscd.securelabsondemand.com.

Note: The results should confirm that the IP address 172.31.0.100 is indeed associated with the storageserver01.securelabsondemand.com system.

8. **Make a screen capture** showing the **results of the reverse DNS query**.

9. **Close** the **Command Prompt window**.

10. In the Firefox browser, **navigate** to **`http://webserver01.securelabsondemand.com`**.

Note: You should be greeted by a 404 Not Found error, generated by a web service: nginx/1.18.0 on a Ubuntu server. In this scenario, that should sound familiar – your team has already configured the web servers to use the expected CSCD society directory as its web root directory, which lives in the default /var/www/ web directory commonly used on Unix-based systems. Because you have yet to mirror the content to either new webserver's own /var/www directory, there is nothing to serve (generally a file called index is looked for in the server's root). You should expect the same for the next server.

11. **Navigate** to **`http://webserver02.securelabsondemand.com`**.

Note: You should be greeted by the same 404 Not Found error. In the next part of the lab, you will resolve these 404 errors.

12. **Close** the **Firefox window**.

Note: Over the course of the next several steps, you will configure the webserver01 and webserver02 sites to become the redundant versions of the master website for the Cure Strange Childhood Diseases Society. Your first task will be to make the site directory reachable via the two web servers. You will accomplish this by sharing it via the NFS protocol.

13. On the DomainController01 desktop, **double-click** the **StorageServer01 PuTTY shortcut** to open a PuTTY session to the Storage server.

Note: You should notice that the command console to the Storage server is using the username "root." PuTTY requires credentials or SSH keys to use a secure shell (SSH) to remotely access another computer. For the lab environment, the Desktop shortcut has been supplied with credentials to seamlessly log you in to the Storage server as the root user. In a production environment, information security management policies should institute strict protocols that disallow automatic remote access to critical servers.

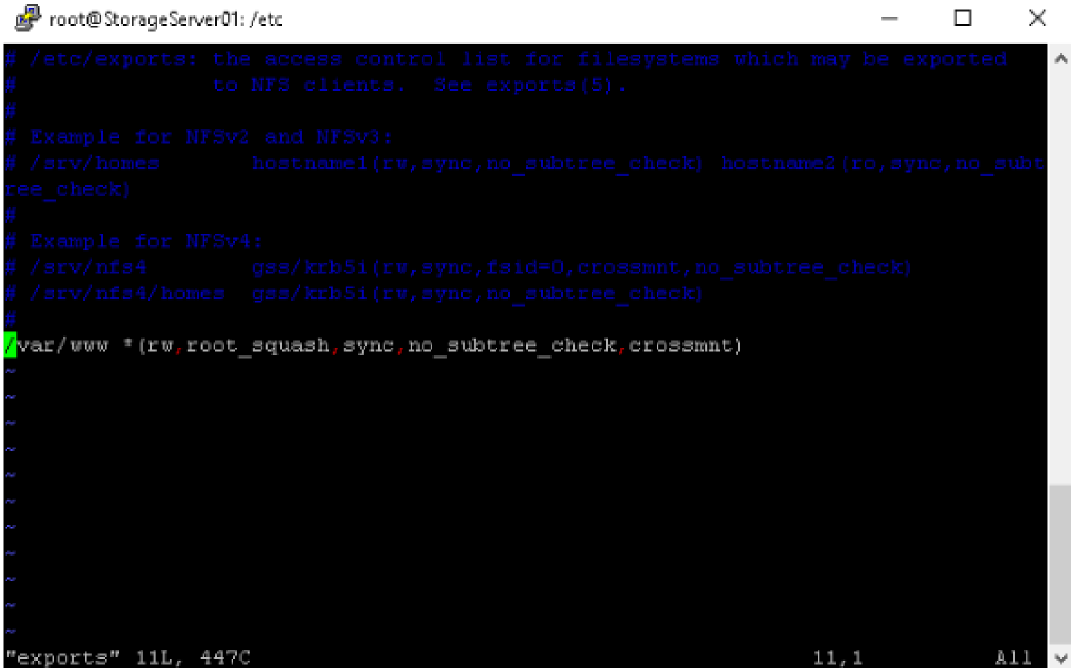
14. At the command prompt, **execute** `cd /etc` to navigate to the /etc directory.

15. At the command prompt, **type** `vi exports` to open the exports file in the vi Editor.

Note: The /etc/exports file instructs Linux which folders to share with NFS and which NFS features should be enabled. In the next steps, you will add a new line of code that instructs Linux to share /var/www with any host via NFS.

16. In the vi Editor, **press o** to add a new line and open edit mode.

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



```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subt
ree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/var/www *(rw,root_squash,sync,no_subtree_check,crossmnt)
~
~
~
~
~
~
~
~
~
~
~
"exports" 11L, 447C                                           11,1          All
```

Edit the exports file

Note: The options used in the /var/www command are described in the following list.

- The asterisk (`*`) is a wild card, in this context meaning that any IP can 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 subdirectories.
- **`crossmnt`** allows multiple client mounts and multiple filesystem mounting.

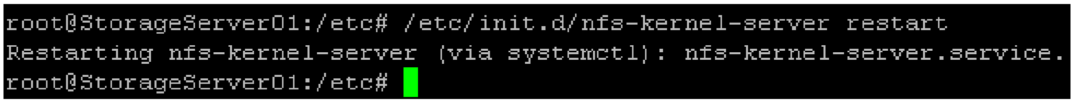
In a production environment, you could follow the [Linux man page for *exports*]() to specify multiple shared directories, and limit access and read/write permission to specific IP addresses (the same is available by typing *man exports* in your Linux terminal).

In the next steps, you will save your changes and restart the NFS server.

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

Note: This changes the configuration file for the NFS server, but does not make the running server actually use those changes. For the changes to take effect, the server must be restarted.

19. At the command prompt, **execute** **`/etc/init.d/nfs-kernel-server restart`** to restart the NFS server on storage.securelabsondemand.com.



```
root@StorageServer01:/etc# /etc/init.d/nfs-kernel-server restart
Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service.
root@StorageServer01:/etc#
```

Restart the NFS server

Note: You should see the message *Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service*, followed by a return to the command prompt. If you see that the restart failed, ensure you have typed the correct information into the exports file (steps 14-18).

20. At the command prompt, **execute** `exit` to close the PuTTY session.

Note: Now that you have configured the storage server to share the */var/www* directory, the Storage server can be referred to as the *NFS server*. Any system that accesses the shared files via NFS can be referred to as an *NFS client*. Over the course of the next several steps, you will configure two web servers as NFS clients. From each web server, you will *mount* the NFS server's */var/www* directory. *Mounting* the shared directory will allow the web servers to access the contents of the NFS server's shared directory as if they are local files and directories on the NFS clients. Mounting a remote filesystem involves an intricate communication system between the client and server systems, the details of which are outside the scope of this lab. For information on how the NFS service works, click here.

21. On the DomainController01 desktop, **double-click** the **WebServer01 shortcut** to open a PuTTY session to the WebServer01 server.

Note: You should notice that the command console to WebServer01 is using the username "root." As with the Storage server, the PuTTY Desktop shortcut has been configured for a seamless connection during the lab.

22. At the command prompt, **execute** `cd /etc` to navigate to the /etc directory.

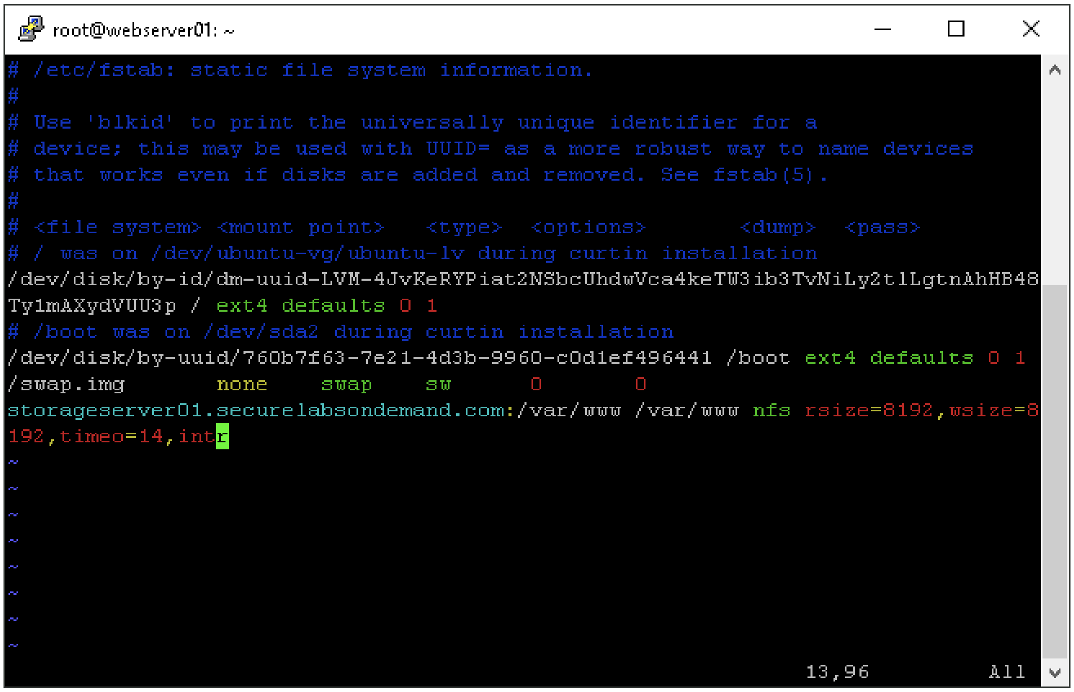
23. At the prompt, **execute `vi fstab`** to open the file systems table in the vi Editor.

Note: You should notice that the lines begin with the # symbol, /dev, or /swap.img. The lines that begin with the # symbol represent comments that are ignored by the NFS server and client. The lines that begin with /dev are the top directory (/) and the /boot filesystem. The /swap.img filesystem reserves hard drive space for RAM-like memory management. The */etc/fstab* file instructs the Linux OS which filesystems should be mounted on startup. At the operating system level, filesystems are simply trees of memory locations which represent files on various branches. By mounting these filesystems, the operating system makes them available at some branch in your local tree/filesystem.

In the next steps, you will add a line that instructs webserver01 to mount the /var/www directory, which you “exported” in the PuTTY session to the Storage server.

24. In the vi Editor, **press o** to add a new line and open edit mode.

25. At the new line, **type `storageserver01.securelabsondemand.com:/var/www /var/www nfs rsize=8192,wsize=8192,timeo=14,intr`**, then **press Esc** to exit edit mode.



```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/ubuntu-vg/ubuntu-lv during curtin installation
/dev/disk/by-id/dm-uuid-LVM-4JvKeRYPiat2NSbcUhdwVca4keTW3ib3TvNiLy2tlLgtnAhHB48
Ty1mAXydVUU3p / ext4 defaults 0 1
# /boot was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/760b7f63-7e21-4d3b-9960-c0d1ef496441 /boot ext4 defaults 0 1
/swap.img       none    swap    sw      0       0
storageserver01.securelabsondemand.com:/var/www /var/www nfs rsize=8192,wsize=8
192,timeo=14,intr
~
~
~
~
~
~
~
~
                                                              13,96         All
```

Edit the fstab file

Note: The options used in the mount command are described in the following list.

- **`storageserver01.securelabsondemand.com:/var/www`** is the NFS server and the directory that is local to the NFS server which you will mount on webserver01; this is called the exported path.
- **`/var/www`** is the local directory on webserver01 that will be used as the mountpoint for the NFS server's exported path.
- **`nfs`** indicates that the mount type is NFS.
- **`rsize=8192`** defines the maximum number of bytes that the NFS client can receive in a read request to the NFS server.
- **`wsize=8192`** defines the maximum number of bytes that the NFS client can send in a write request to the NFS server.
- **`timeo=14`** defines the time, in tenths of a second, that the NFS client will wait to retry a request of the NFS server should a request go unanswered.
- **`intr`** allows NFS requests to be interrupted; in other words, if an NFS server is unreachable, the client will wait until the server is reachable again, then continue its requests.

Direct your attention to the first and second phrases in this line. Essentially, they are each /var/www – the first is on storageserver01's local filesystem and the second is on webserver01's local filesystem. It is possible to use a mountpoint that is named differently than the NFS server's exported path. However, your intent in this lab is to mirror the web server directory structure, which is /var/www by default with most web servers.

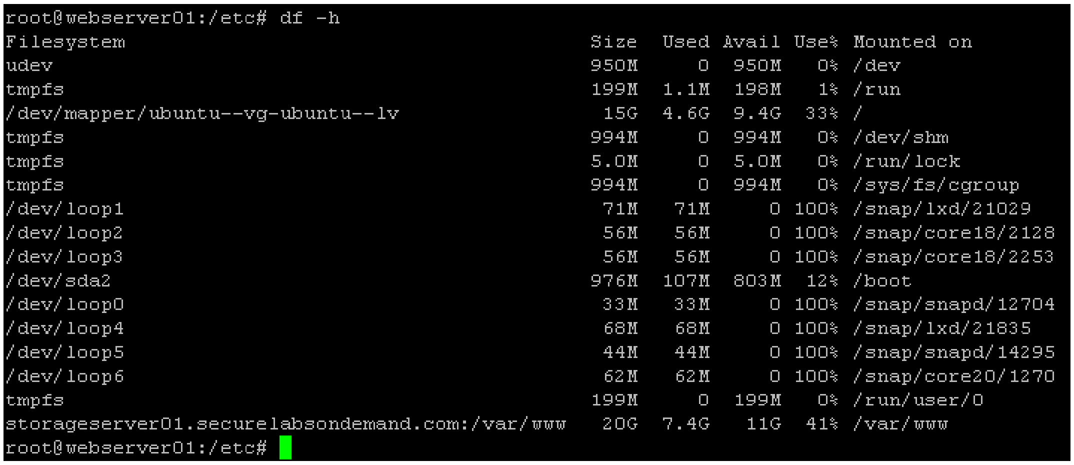
In the next steps, you will save your changes to the filesystem table (fstab) configuration file. You will then mount your new NFS share, confirm that mount is successful, and then apply the same treatment to the remaining web server.

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

27. At the command prompt, **execute** `mount -av` to mount the storage server.

Note: You should see a list of mounted filesystems. The bottom line should read that /var/www has been successfully mounted, while the two lines above that should confirm the options that you set for read/write sizes and handling timeouts.

28. At the command prompt, **execute** `df -h` to verify that the storage server has been mounted correctly.



```
root@webserver01:/etc# df -h
Filesystem                                      Size  Used Avail Use% Mounted on
udev                                            950M     0  950M   0% /dev
tmpfs                                           199M  1.1M  198M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv                15G  4.6G  9.4G  33% /
tmpfs                                           994M     0  994M   0% /dev/shm
tmpfs                                           5.0M     0  5.0M   0% /run/lock
tmpfs                                           994M     0  994M   0% /sys/fs/cgroup
/dev/loop1                                       71M   71M     0 100% /snap/lxd/21029
/dev/loop2                                       56M   56M     0 100% /snap/core18/2128
/dev/loop3                                       56M   56M     0 100% /snap/core18/2253
/dev/sda2                                       976M  107M  803M  12% /boot
/dev/loop0                                       33M   33M     0 100% /snap/snapd/12704
/dev/loop4                                       68M   68M     0 100% /snap/lxd/21835
/dev/loop5                                       44M   44M     0 100% /snap/snapd/14295
/dev/loop6                                       62M   62M     0 100% /snap/core20/1270
tmpfs                                           199M     0  199M   0% /run/user/0
storageserver01.securelabsondemand.com:/var/www   20G  7.4G   11G  41% /var/www
root@webserver01:/etc#
```

Verify the storage server is mounted

Note: You should see a text-based table with columns of Filesystem, Size, Used, Avail, Use%, and Mounted on. The bottom line should indicate that the Filesystem storageserver01.securelabsondemand.com:/var/www is of Size 20G, with 7.4G Used and 11G Avail(able) for 41% Use%, and that it is Mounted (locally) on /var/www.

29. At the command prompt, **execute** `exit` to close the PuTTY session.

30. On the DomainController01 desktop, **double-click** the **WebServer02 shortcut** to open a PuTTY session to the WebServer02 server.

31. **Repeat steps 22-29** for the WebServer02 server (172.30.0.102).

Note: You have now configured both webserver01 and webserver02 to be NFS clients that use the same NFS folder on the storage server. In the next steps, you will confirm that your changes were successful. Recall that your previous visits to webserver01 and webserver01 via Firefox confirmed that they were each running a web server, but neither were serving web pages. By mounting the Storage server's /var/www directory at the same-named local directory on each web server, their NGINX web servers should now have files to serve when requested. Namely, it should show the same webpage that you previously viewed on the Storage server.

32. **Open** a **new Firefox window**.

33. **Navigate** to `http://webserver01.securelabsondemand.com`.

34. **Make a screen capture** showing the **updated webserver01 home page**.

35. **Navigate** to `http://webserver02.securelabsondemand.com`.

36. **Make a screen capture** showing the **updated webserver02 home page**.

Part 2: Configure Load Balancing

Note: In this part of the lab, you will configure the pfSense firewall/router to load balance all traffic to the CSCD website across the two redundant web servers. *Load balancing* is a networking solution that distributes traffic across multiple servers in a server group. It is a key component of highly-available (HA) services, which can be used to ensure their availability. An organization's BCP or DRP may use redundancy and load balancing for systems whose acceptable minimum down time is very little or none at all.

Here you will use HAproxy, which is a pfSense package that manages load balancing and consists of a front-end (IP address on which to listen) and a back-end (redundant web servers). You will configure HAproxy on the local pfSense firewall-router in the lab topology, which is responsible for routing and filtering public traffic to your web servers. Note that the perimeter firewall is used for load-balancing in this scenario only for lab economy, while best practice would dictate constructing a dedicated load-balancer.

In the next steps, you will use access the pfSense webGUI (graphical user interface) and configure the HAproxy package.

1. In the Firefox window, **navigate** to **`172.16.0.1`** to access the pfSense web GUI.

2. At the pfSense login page, **log in** using the following credentials:

   User: **`admin`**
   Password: **`pfsense`**

Note: You should see the pfSense Dashboard. It provides system and services overview on the firewall, including the system and user information, BIOS, CPU Type, and Uptime. In the pane on the right, you should also see that this pfSense firewall services a WAN, LAN, and DMZ, as well as its IP address on their respective interfaces.

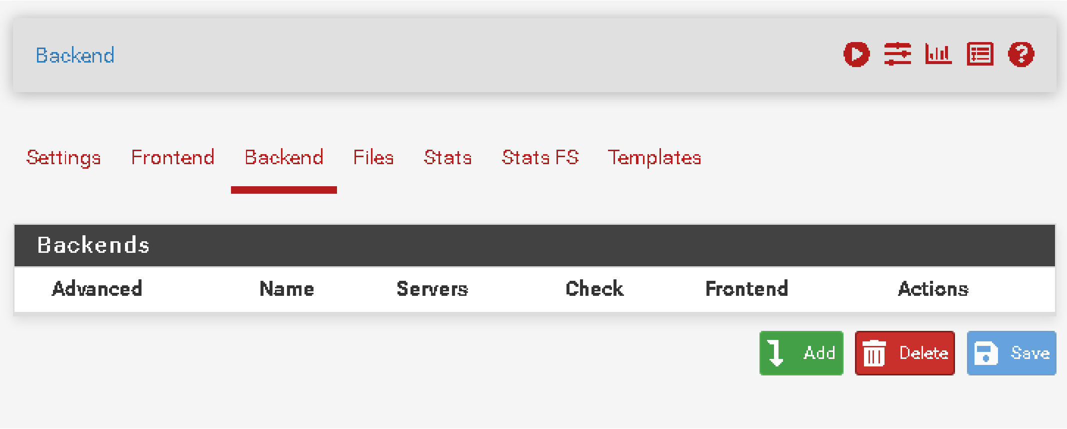
The pfSense firewall has an interface on the LAN (local area network), which contains your internal machines, which are generally inaccessible outside of the organization (like the DomainController01 machine you are currently using); an interface on the WAN (wide area network) which represents the start of the public Internet (generally, the connection to your ISP’s facilities); and the DMZ, which contains your web servers, and is generally made more accessible to the public, as it contains resources intended for partial exposure to external networks. Access to any of these three networks is determined by the interface the traffic is coming in on. This means that for all requests from public users, the WAN interface will be responsible for guiding that traffic to the DMZ, and deciding which of your two web servers gets that traffic.

Over the next steps, you will set-up HAProxy in pfSense to emulate decision-making for traffic requests to the redundant web servers so that they appear as one web server to users.

3. From the pfSense menu bar, **navigate** to **Services > HAProxy**.

Note: *HAProxy is divided into a backend and frontend component.* The Backend of HAProxy creates a pool of redundant web servers, to which the Frontend will direct traffic. Thus, you will set up the Backend before you set up the Frontend. The Frontend handles exposure of the web server pool to the Internet so that multiple servers can be referred to in the background without the user having to use different IP addresses / domain names. By connecting the Backend to the Frontend, the pfSense firewall will become a load-balancer.

4. On the Services / HAProxy / Frontend page, **click** the **Backend tab** to open the Backend page.



Services / HAProxy / Backend

5. On the Backend page, **click** the **Add button** to begin the process of adding a backend for your load-balancer.

6. In the Edit HAProxy Backend server pool module, **type** **`http_server_pool`** in the Name field.

7. In the Server list, **click** the **down arrow** to add a new server entry.

Note: Most information here can be left alone, as it concerns certificate configuration for HTTPS (encrypted HTTP) deployments. In general, HTTPS is recommended, and should be considered a necessary upgrade (or pre-launch requirement), but you will use HTTP for simplicity in this lab.

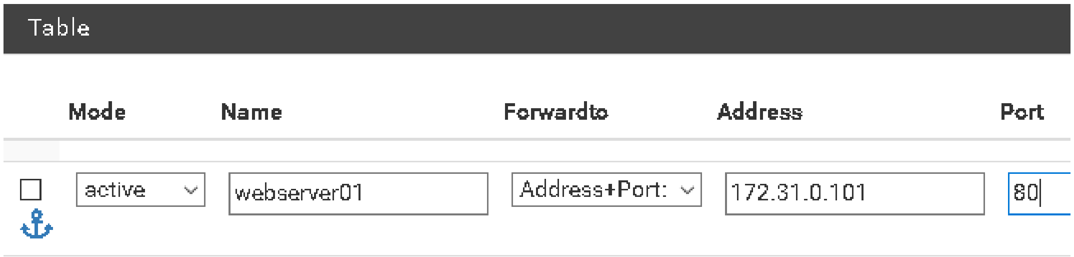
Two other options are worth noting here, the first being Mode. You will leave Mode for both servers to Active, which specifies that both should receive incoming traffic, but the other options available provide good contrast to such a typical load-balancing scenario. For example, you may opt for an Active/Standby arrangement, which would instead dictate that all traffic would be directed to the Active server until it fails; then the Standby server would become the Active server and take over website serving responsibilities. Such load-balancing and fail-over considerations are crucial in achieving a high-availability (HA) deployment.

The other option is weight, which you may need to horizontally scroll the Server List table to see. This is a hyperparameter (does not necessarily correspond to any hard metrics) that can be adjusted for each server, and provides the option to prioritize servers for smarter balancing. Both of the web servers in this environment are equally performant Ubuntu Linux machines with identical configurations, so no weight adjustments are necessary.

You can see more detailed information about these fields by clicking the Field explanations icon.

8. **Complete** the new server fields using the following information:

   Name: **`webserver01`**
   Address: **`172.31.0.101`**
   Port: **`80`**



Table

	Mode	Name	Forwardto	Address	Port
☐ ⚓	active	webserver01	Address+Port:	172.31.0.101	80

Server list

9. **Repeat steps 7-8** using the following information to add webserver02 to the pool.

   Name: **`webserver02`**
   Address: **`172.31.0.102`**
   Port: **`80`**

10. **Scroll down** to the **Loadbalancing options module**, then **click** the **Plus icon** to expand it.

Note: You have specified Active/Active, which leaves one configuration question to answer: how do you want to divvy up that activity? You should see a list of options that includes *Round Robin*, *Static Round Robin*, *Least connections*, *Source*, and *Uri (HTTP backends only)*. The *Round Robin options* share resources by taking turns on each connection according to an administrator-defined weight (i.e., servers with higher weights will receive a proportionately higher workload). The *Least connections option* shares resources based on the number of server connections and is useful for HTTPS, SQL, and other services which may use longer connections.

11. **Select** the **Static Round Robin radio button**.

Note: This version of the Round Robin will share resources by taking equal turns.

12. **Scroll down** to the **Health checking module**, then **select Basic** from the Health check method menu.

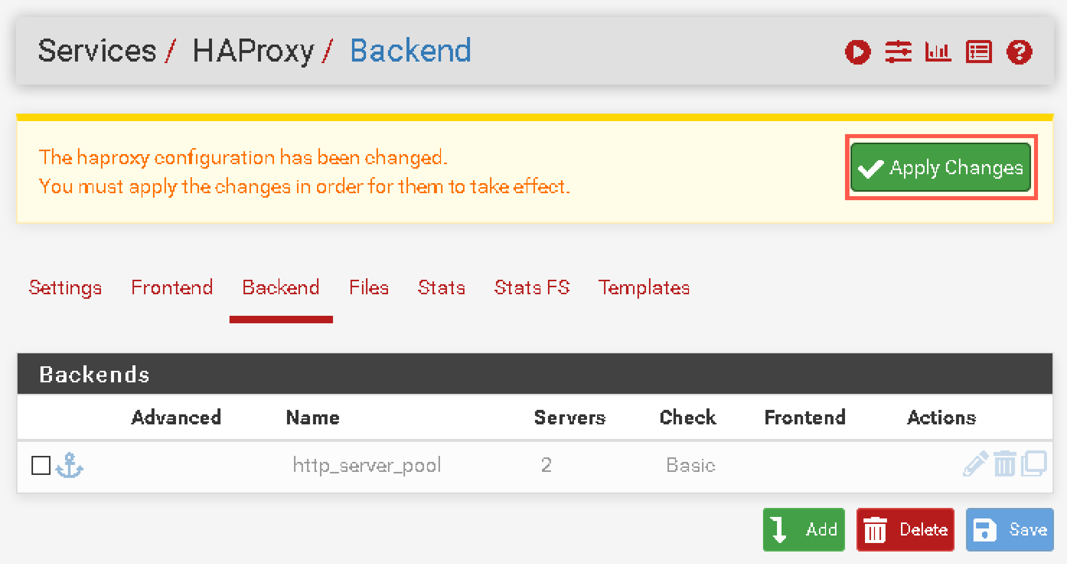
Note: If you intend to perform failover as part of a highly-available deployment (the HA in HAProxy) – that is, a deployment that can provide near-continuous service in the event of one or more failures – then you need a way of monitoring service health, and thereby determine when a 'failure' occurs. Your initial configuration will only provide load-balancing, but your BCP and DRP include implementing high-availability through health monitoring and failover at a later date.

Selecting Basic (meaning a basic layer 4 check over TCP) without specifying a frequency results in no check being performed. As a result, the servers will always be considered up, with no failure triggers.

There are numerous protocols available for performing health queries since HAProxy provides high-availability options for a range of deployment types, not just web services. This includes email, authentication, and database server deployments.

13. At the bottom of the page, **click** the **Save button** to save your changes and return to the Services HAProxy / Backend page.

14. **Click** the **Apply Changes button** to push your changes to the running firewall configuration.



The haproxy configuration has been changed.
You must apply the changes in order for them to take effect.

Backends

	Advanced	Name	Servers	Check	Frontend	Actions
□ ⚓		http_server_pool	2	Basic		

Apply changes

15. **Make a screen capture** showing the **http_server_pool backend.**

Note: Now that the Backend is configured, you will configure the Frontend to accept connections at one IP address, which pfSense will load-balance via your Backend configuration.

16. **Click** the **Frontend tab** to return to the Frontend page.

17. On the Frontend page, **click** the **Add button** to begin the process of adding a backend for your load-balancer.

Note: Your main objective here is to specify the IP / interface that will represent the web server pool. You could use the device's own public IP address (the IP on this pfSense firewall's WAN interface), which there may be a good case for if this were a dedicated device. Public-facing IP addresses are not freely available. For a production site, you would have a range of addresses provided by your ISP. The number of addresses you have available would contribute to your allocation decisions. For this lab, you will instead use an IP alias assigned to the WAN interface. This IP address will be used to publicly represent and serve your load-balanced web servers. In order for HAProxy to act as a load balancer, the IP address must resolve to WAN interface so that requests from the general internet will be received there.

18. In the Edit HAProxy Frontend section, **type** the following information:

    Name: **`http_access`**
    Description: **`Access to http_server_pool`**
    Listen address: **203.30.3.100 (Public IP for CSCD Society)**

19. **Scroll down** to the **Default backend module** and **select http_server_pool** from the default Backend menu.

20. At the bottom of the page, **click** the **Save button** to save your changes and return to the Services HAProxy / Frontend page.

21. **Click** the **Apply Changes button** to push your changes to the running firewall configuration.

22. **Make a screen capture** showing the **http_access frontend**.

23. **Click** the **Settings tab** to open the HAProxy Settings page.

24. In the General settings module, **click** the **Enable HAProxy checkbox** and **set** the **Maximum connections** to **`1000`** per process.

25. Scroll down to the Stats tab module, then **type** **`2200`** in the Internal stats port field.

26. At the bottom of the page, **click** the **Save button** to save your changes.

27. **Click** the **Apply Changes button** to push your changes to the running firewall configuration.

Note: You will need to make one final update before HAProxy is ready for production. Recall that the firewall is acting as the authoritative domain name server for this website, but the name record for the production site, cscd.securelabsondemand.com, is currently pointing to the storageserver01 in the DMZ (172.31.0.100) in the DMZ. Now that you have configured load balancing at the web servers public IP, you can edit the DNS record to point to this address.

28. From the pfSense menu bar, **navigate** to **Services > DNS Resolver**.

29. **Scroll down** to the **Host Overrides module**.

Note: There are three entries here, all for the securelabsondemand.com domain. You are looking for the Cure Strange Childhood Diseases host, which is publicly known by the hostname/subdomain *cscd*.

30. **Click** the **pencil icon** to the right of the cscd.securelabsondemand.com entry to open the Edit Host Override page.

31. On the Edit Host Override page, **change** the IP Address to **`203.30.3.100`**, the public IP assigned to your HAProxy frontend.

32. At the bottom of the page, **click** the **Save button** to save your changes and return to the Services HAProxy / General settings page.

33. **Click** the **Apply Changes button** to push your changes to the running firewall configuration. The change may take up to a minute to apply.

34. **Scroll down** to the **Host Overrides module**.

35. **Make a screen capture** showing the **new Host Overrides entry for cscd.securelabsondemand.com**.

Note: Do not close the Firefox window.

Part 3: Verify Load Balancing

Note: In this part of the lab, you will verify that your load-balancing configuration is functioning as expected. In a production environment, you should track request counts, active connection or active flow counts, error rates, latency, number of healthy/unhealthy hosts, and the count of rejected/failed connections. You can read more about load balancing metrics here. For the purposes of this lab, you will use HAProxy stats to measure whether your load-balancing configuration is functioning as you have intended.

In the next steps, you will clear your systems DNS cache to ensure you are retrieving the updated DNS record for the website. You will then execute another DNS query to verify that the cscd DNS record is actually pointing at the new load balancer frontend IP address.

1. **Open** a new **Command Prompt window**.

2. At the command prompt, **execute** `ipconfig /flushdns` to clear all existing name records from your DNS cache.

Note: You may have updated the website's record on your DNS resolver, but the vWorkstation may still have records referring to the previous IP in its DNS cache. Answers to recent DNS queries are stored here to avoid repeated lookups, so these records will always be preferred to bugging a DNS resolver again. While these records will expire on their own, they may also be manually flushed to force a new DNS query the next time you make a request to that domain name.

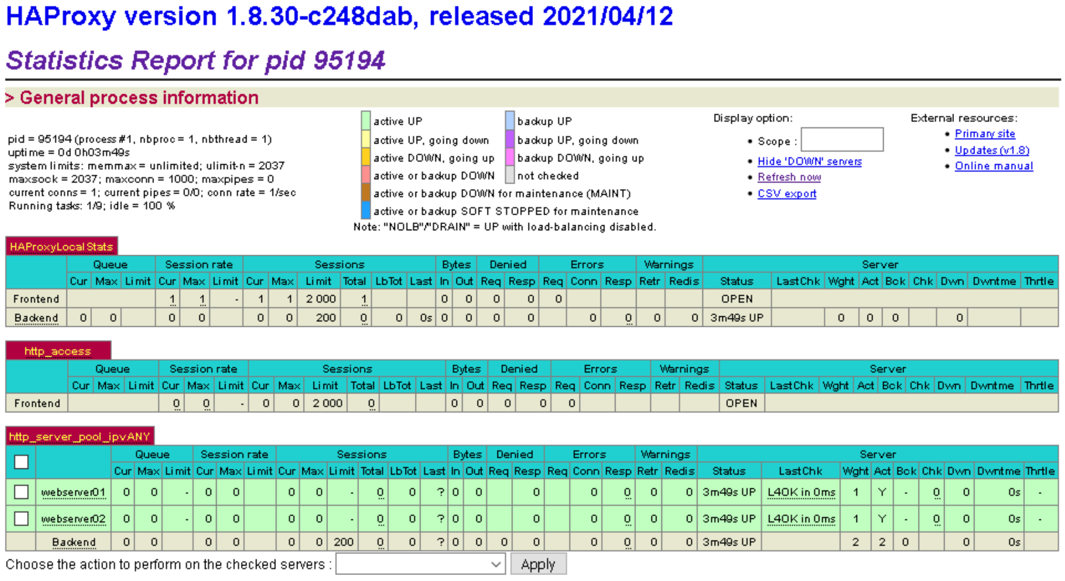
3. At the command prompt, **execute** `nslookup cscd.securelabsondemand.com` to resolve the IP address using the default DNS server.

Note: The pfSense firewall should now report your changes – cscd.securelabsondemand.com resolves to 203.30.3.100. Recall that it was previously resolving to the internal (and private, or RFC1918, non-routable) IP address for the storageserver01.securelabsondemand.com machine (your new NFS server). Normally, as part of clean-up, the existing web service packages and dependencies should be removed from storagerserver01 to limit its functionality to its specific purpose. For the purposes of this lab, you will skip these hygiene steps.

4. **Make a screen capture** showing the **result of your DNS query for cscd.securelabsondemand.com**.

5. In the pfSense webGUI, **navigate** to **Services > HAProxy**.

6. On the Services / HAProxy / Frontend page, **click** the **Stats FS tab** to open the Statistics Report.



HAProxy version 1.8.30-c248dab, released 2021/04/12

Statistics Report for pid 95194

> General process information

pid = 95194 (process #1, nbproc = 1, nbthread = 1)
uptime = 0d 0h03m49s
system limits: memmax = unlimited; ulimit-n = 2037
maxsock = 2037; maxconn = 1000; maxpipes = 0
current conns = 1; current pipes = 0/0; conn rate = 1/sec
Running tasks: 1/9; idle = 100 %

🟩 active UP	🟦 backup UP
🟨 active UP, going down	🟪 backup UP, going down
🟧 active DOWN, going up	🟪 backup DOWN, going up
🟥 active or backup DOWN	⬜ not checked
🟫 active or backup DOWN for maintenance (MAINT)	
🟦 active or backup SOFT STOPPED for maintenance	

Note: "NOLB"/"DRAIN" = UP with load-balancing disabled.

Display option:
- Scope :
- Hide 'DOWN' servers
- Refresh now
- CSV export

External resources:
- Primary site
- Updates (v1.8)
- Online manual

HAProxyLocalStats

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				1	1	-	1	1	2 000	1			0	0	0	0	0					OPEN								
Backend	0	0		0	0		0	0	200	0	0	0s	0	0	0	0		0	0	0	0	3m49s UP		0	0	0		0		

http_access

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				0	0	-	0	0	2 000	0			0	0	0	0	0					OPEN								

http_server_pool_ipvANY

☐		Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
		Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
☐	webserver01	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	3m49s UP	L4OK in 0ms	1	Y	-	0	0	0s	-
☐	webserver02	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	3m49s UP	L4OK in 0ms	1	Y	-	0	0	0s	-
	Backend	0	0		0	0		0	0	200	0	0	?	0	0	0	0		0	0	0	0	3m49s UP		2	2	0		0	0s	

Choose the action to perform on the checked servers : Apply

Statistics Report

Note: You should see General process information in the top section of the page, as well as three tables with statistics for HAProxyLocalStats, http_access, and http_server_pool_ipvANY. You should notice that the *Sessions* > *Total* column of the *http_server_pool_ipvANY* (bottom) box currently displays counts of 0 in each row. This column will reflect the number of HTTP requests made to the servers in the pool. Recall that you selected Static Round Robin as the method. Since you also weighted both of these servers equally (by neglecting to weight them, leaving a default of 1 for each), each new request should be given to the next server in line: first webserver01, then webserver02, then webserver01, then webserver02, and so on...

In the next steps, you will access the website via the Frontend, then confirm that the Round Robin Backend load-balancing is functioning as expected.

7. From the DomainController01 taskbar, **open** the **Chrome browser** and **navigate** to `http://cscd.securelabsondemand.com`. If the website does not load on the first try, wait 30 seconds and try again.

8. In the Chrome browser, **refresh** the **page to access the website twice.**

9. **Restore** the **Firefox window**.

10. In the Firefox browser, **refresh** the **Statistics Report page** to update the report.

11. **Make a screen capture** showing the **Statistics Report with a value of at least 1 in the Sessions > Total column of the http_server_pool_ipvANY box, for both webserver01 and webserver02.**

12. **Close** any **open windows**.

Note: This concludes Section 2 of the lab.

Section 3: Challenge and Analysis

Note: The following exercises are provided to allow independent, unguided work using the skills you learned earlier in this lab - similar to what you would encounter in a real-world situation.

Part 1: Add Failover Functionality

For the purposes of this exercise, you will continue the work you started in Section 2, where you began the process of configuring the CSCD website for high availability. Although you can now add “configured a load-balancer to scale web server fleet” to your resume, your deployment is fairly minimal, and not worthy being considered High Availability yet.

To make your deployment highly-available, you will need to add some health checks. You may recall that you had an opportunity to do this during your initial load balancer set-up, when you opted for a *Basic* check (using the TCP protocol) and an unspecified *Check frequency*. This combination means no check will be performed and the servers are always considered up. For this exercise, your objective is to alter this configuration so that a Basic TCP check is performed every 10 seconds.

Using the pfSense webGUI, update the HAProxy backend to perform a Basic (TCP / layer 4) health check every 10 seconds.

Hint: *The health check is performed on your web server nodes in the backend of your deployment, so you will want to look for something about Health checking in its configuration. Also, don’t forget to convert to the appropriate units for your Check frequency so that you get 10 seconds for each.*

Make a screen capture showing the **updated Check Frequency value in the Health checking module**.

Part 2: Validate Failover Functionality

Now that you’ve updated HAProxy to perform regular health checks, you will need to test your changes to confirm that the regular health checks produce the expected result in the event that one of the web servers goes down.

In this exercise, you will force one of these web servers to fail the TCP check you configured in Part 1. Because HTTP relies on TCP for site connections, taking down the web service itself on either WebServer01 or WebServer02 is sufficient.

Connect to either WebServer01 or WebServer02 via the appropriate PuTTY shortcut on DomainController01, then **execute** `service nginx stop` to shut down the web service. Next, navigate to the HAProxy Statistics Report and confirm one of the servers in http_server_pool is now being reported as down (you have to refresh, and give it at least 10 seconds per your configuration in Part 1). Once you’ve confirmed one of the servers is being reported as down, open a new Chrome browser tab and navigate to cscd.securelabsondemand.com, then begin reloading the page to generate additional sessions. The HAProxy stats page should show that the number of total sessions (http_server_pool_ipvANY, Sessions > Total) for the DOWN node will have stopped increasing with each additional session, while the remaining UP node will continue to receive each new session you generate.

Make a screen capture showing the **HAProxy Statistics Report with a host in a DOWN state, as well as the UP host having more total sessions (http_server_pool_ipvANY, Sessions > Total) than the DOWN host**.

Note: This concludes Section 3 of the lab.