

Configuring Backup and Recovery Functions (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 09

Student:
Patrick Kierzkowski

Email:
pxk405@francis.edu

Time on Task:
18 hours, 51 minutes

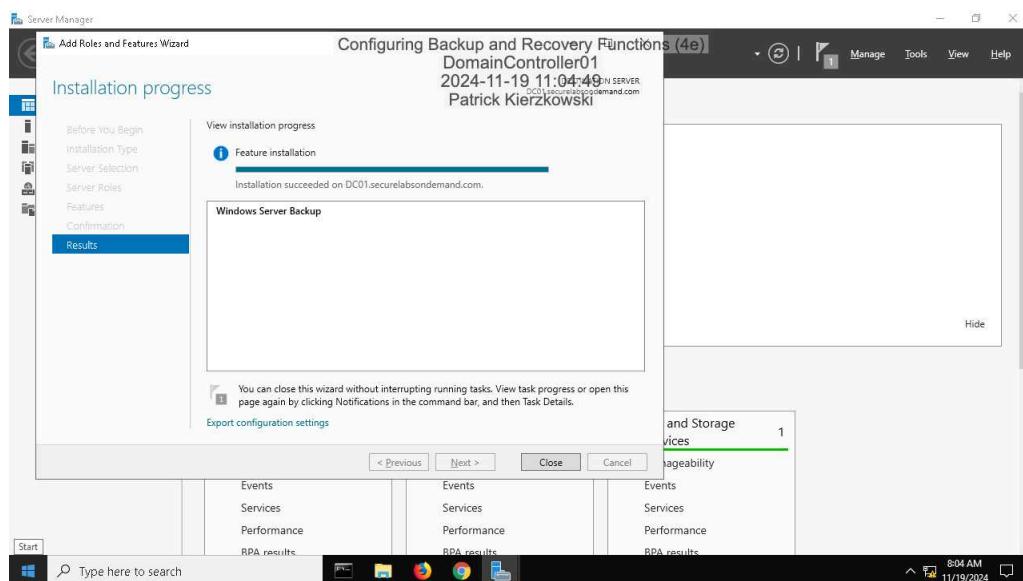
Progress:
100%

Report Generated: Monday, July 7, 2025 at 9:51 PM

Section 1: Hands-On Demonstration

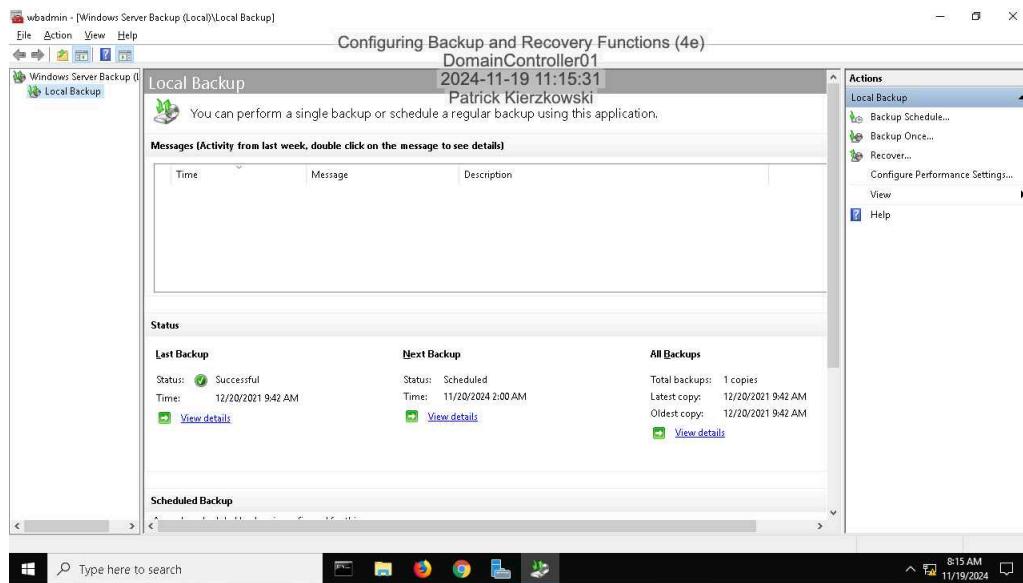
Part 1: Install Windows Server Backup

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



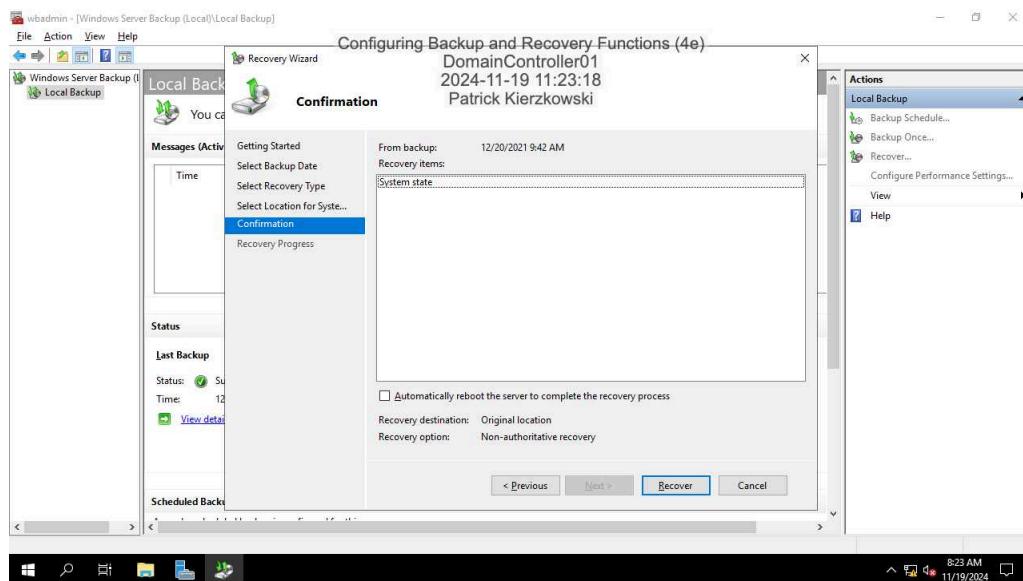
Part 2: Configure a System State Backup

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



Part 3: Restore from a System State Backup

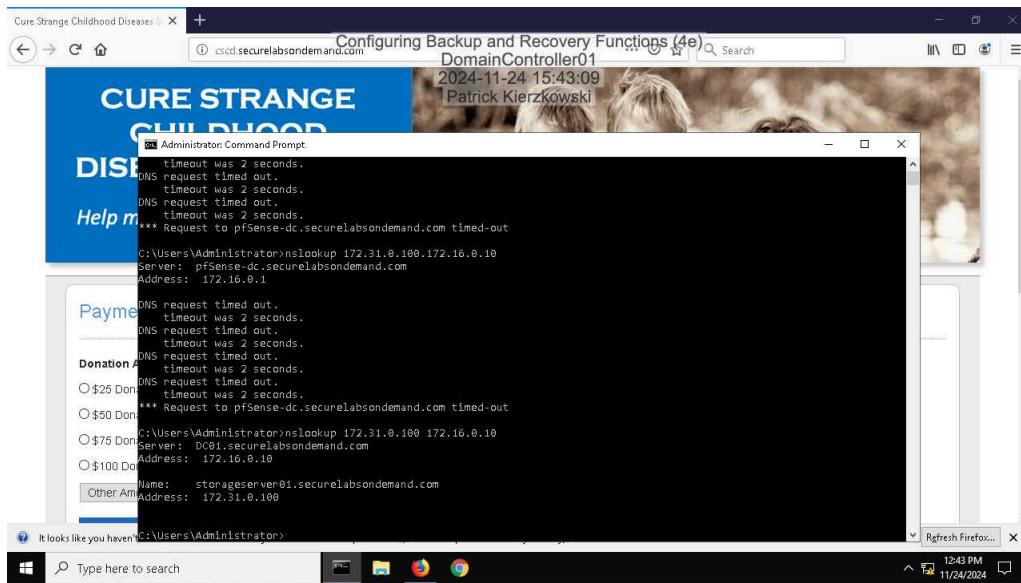
15. Make a screen capture showing the **Recovery Wizard Confirmation page**.



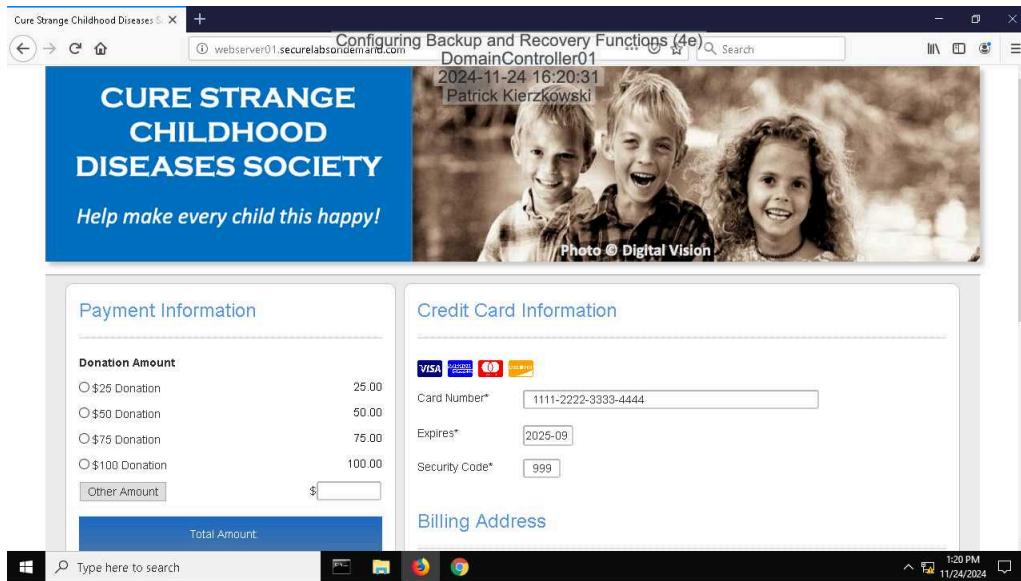
Section 2: Applied Learning

Part 1: Configure an NFS Share

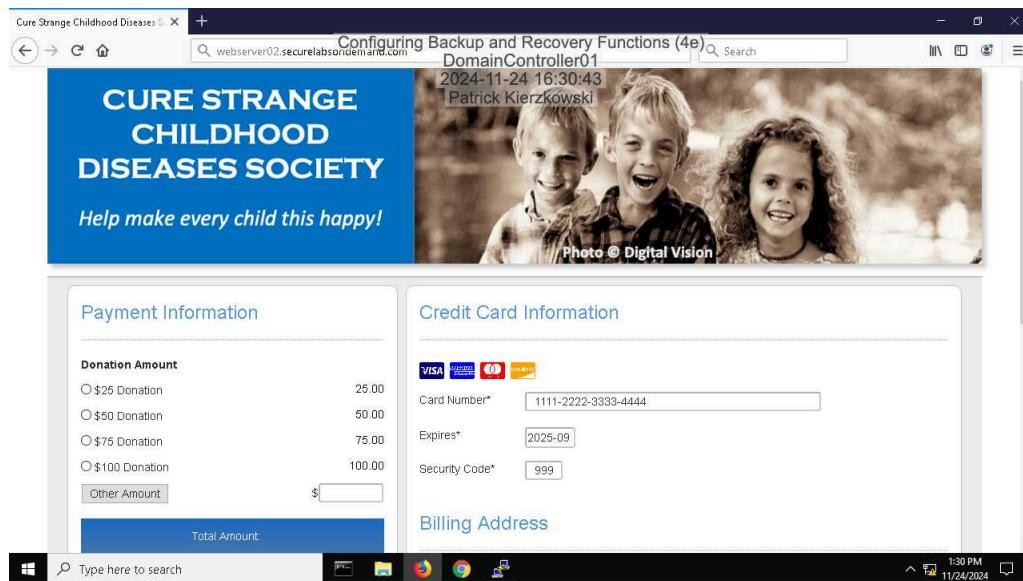
- 8. Make a screen capture showing the results of the reverse DNS query.**



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

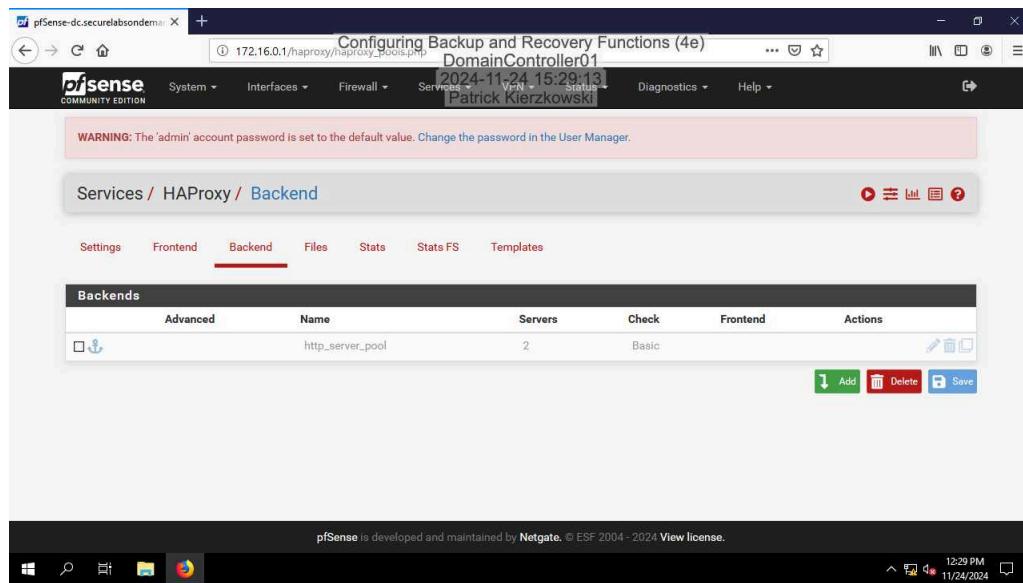


36. Make a screen capture showing the updated webserver02 home page.



Part 2: Configure Load Balancing

15. Make a screen capture showing the http_server_pool backend.



22. Make a screen capture showing the http_access frontend.

The screenshot shows the pfSense web interface at 172.16.0.1/haproxy/listeners.php. The title bar says "Configuring Backup and Recovery Functions (4e)" and the URL bar shows "172.16.0.1/haproxy/listeners.php". The top navigation bar includes "System", "Interfaces", "Firewall", "Services", "Status", "Diagnostics", and "Help". The user "Patrick Kierzkowski" is logged in. A red warning message in a box states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the page title is "Services / HAProxy / Frontend". The main content area has tabs for "Settings", "Frontend" (which is selected), "Backend", "Files", "Stats", "Stats FS", and "Templates". A table titled "Frontends" lists one entry: "http_access" (Primary, Shared, On, Advanced), Name: "http_access", Description: "Access to http_server_pool", Address: "203.30.3.100:80", Type: "http", Backend: "http_server_pool (default)". Action buttons include edit, delete, and save. At the bottom of the table are "Add", "Delete", and "Save" buttons. The pfSense footer at the bottom left says "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license." and the bottom right shows the date and time as "11/24/2024 12:31 PM".

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

The screenshot shows the pfSense web interface at 172.16.0.1/services_unbound.php. The title bar says "Configuring Backup and Recovery Functions (4e)" and the URL bar shows "172.16.0.1/services_unbound.php". The top navigation bar includes "System", "Interfaces", "Firewall", "Services", "Status", "Diagnostics", and "Help". The user "Patrick Kierzkowski" is logged in. A table titled "Host Overrides" lists three entries: "cscd" (Host), "securelabsondemand.com" (Parent domain of host), "203.30.3.100" (IP to return), "CSCD Society production site" (Description). Action buttons include edit, delete, and add. Below the table is a note: "Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'ns.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records." A green "Add" button is visible. The pfSense footer at the bottom left says "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license." and the bottom right shows the date and time as "11/24/2024 12:34 PM".

Part 3: Verify Load Balancing

Configuring Backup and Recovery Functions (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 09

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2098]
(c) 2018 Microsoft Corporation. All rights reserved.
DomainController01 | 2024-11-24 16:39:13
C:\Users\Administrator>ipconfig/flushdns
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

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: 203.30.3.100

C:\Users\Administrator>
```

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'has.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.

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`.

Statistics Report for HAProxy

Configuring Backup and Recovery Functions (4e) DomainController01 | 2024-11-24 16:54:21 | Patrick Kierzkowski

HAProxy version 1.8.30-c248dab, released 2021/04/11

Statistics Report for pid 91904

> General process information

pid = 91904 (process #1, nbproc = 1, nthread = 1)	uptime = 0d 00m 03s
systems limits: memmax = unlimited, ultimn = 2037	maxconn = 2037, maxconn = 1000, maxspies = 0
current conn = 1, current pipes = 0, conn rate = 1/sec	Running task: 100 idle = 100 %

Note: "NOLB" or "BRAIN" = UP with load balancing disabled.

> General process information

Queue		Session rate		Sessions		Bytes		Denied		Errors		Warnings		Status		LastChk		Weight		Act		Bck		Chk		Dwn		Downtime		Throttle	
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Req	Ref	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtime	Throttle		
Frontend	1	1	-	1	1	2	0	0	6		675	108,067	0	0	0	0	0	0	0	0	OPEN										
Backend	0	0	0	0	0	0	200	0	0	0	0	675	108,067	0	0	0	0	0	0	0	0	2m3s UP		0	0	0	0	0	0	0	0

> http_access

Queue		Session rate		Sessions		Bytes		Denied		Errors		Warnings		Status		LastChk		Weight		Act		Bck		Chk		Dwn		Downtime		Throttle	
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Req	Ref	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtime	Throttle		
Frontend	0	5	-	0	5	2	0	0	2,000	7	6,895	642,691	0	0	0	0	0	0	0	0	OPEN										

> http_server_pool_ipvANY

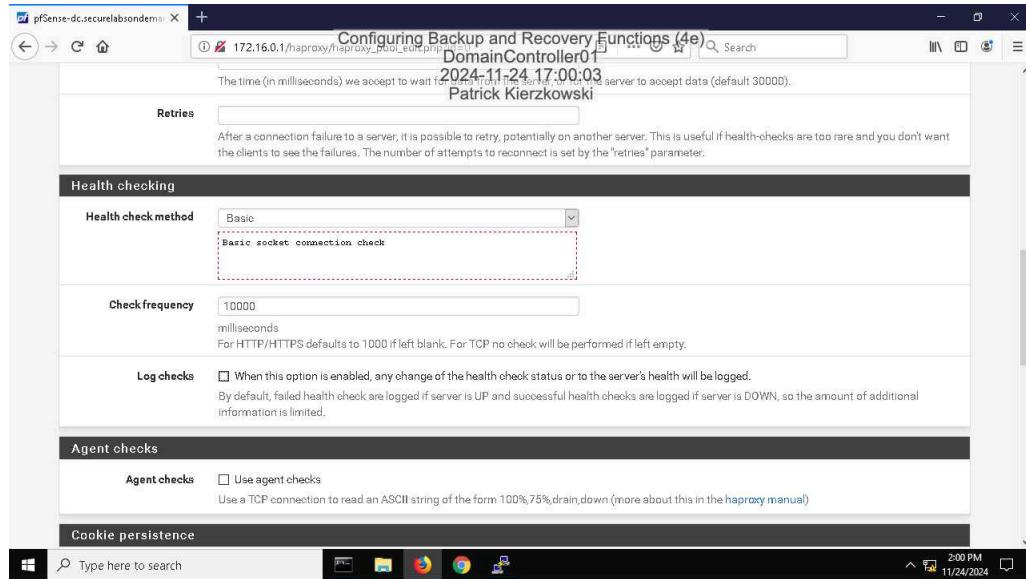
Queue		Session rate		Sessions		Bytes		Denied		Errors		Warnings		Status		LastChk		Weight		Act		Bck		Chk		Dwn		Downtime		Throttle	
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Req	Ref	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtime	Throttle		
webserver01	0	0	-	0	5	0	2	-	8	8	1m21s	3,078	639,947	0	0	0	0	0	0	0	2m13s UP	L40K in 0ms	1	Y	-	0	0	0	0s	-	
webserver02	0	0	-	0	4	0	2	-	7	7	1m21s	3,219	2,744	0	0	0	0	0	0	0	2m13s UP	L40K in 0ms	1	Y	-	0	0	0	0s	-	
Backend	0	0	0	0	0	0	3	200	15	16	1m21s	6,890	642,691	0	0	0	0	0	0	0	2m13s UP		2	2	0	0	0	0	0s		

Choose the action to perform on the checked servers:

Section 3: Challenge and Analysis

Part 1: Add Failover Functionality

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



Part 2: Validate Failover Functionality

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.

