Apache HTTP Server Configuration on Non-Default Port

Overview

This project documents the configuration of the Apache HTTP Server to run on a non-default port (8001) in a secured Linux environment. The workflow demonstrates how application configuration, SELinux enforcement, firewall rules, and service validation work together to safely expose a web service.

What Was Done

Modified the Apache configuration file to change the listening port from the default (80) to 8001

Verified and configured SELinux to allow Apache to bind to the new port using the appropriate http_port_t context

Updated firewall rules to permit inbound TCP traffic on port 8001

Restarted the Apache service to apply configuration changes

Confirmed the service was active and running without errors

Validated successful access to the web service using curl on the new port

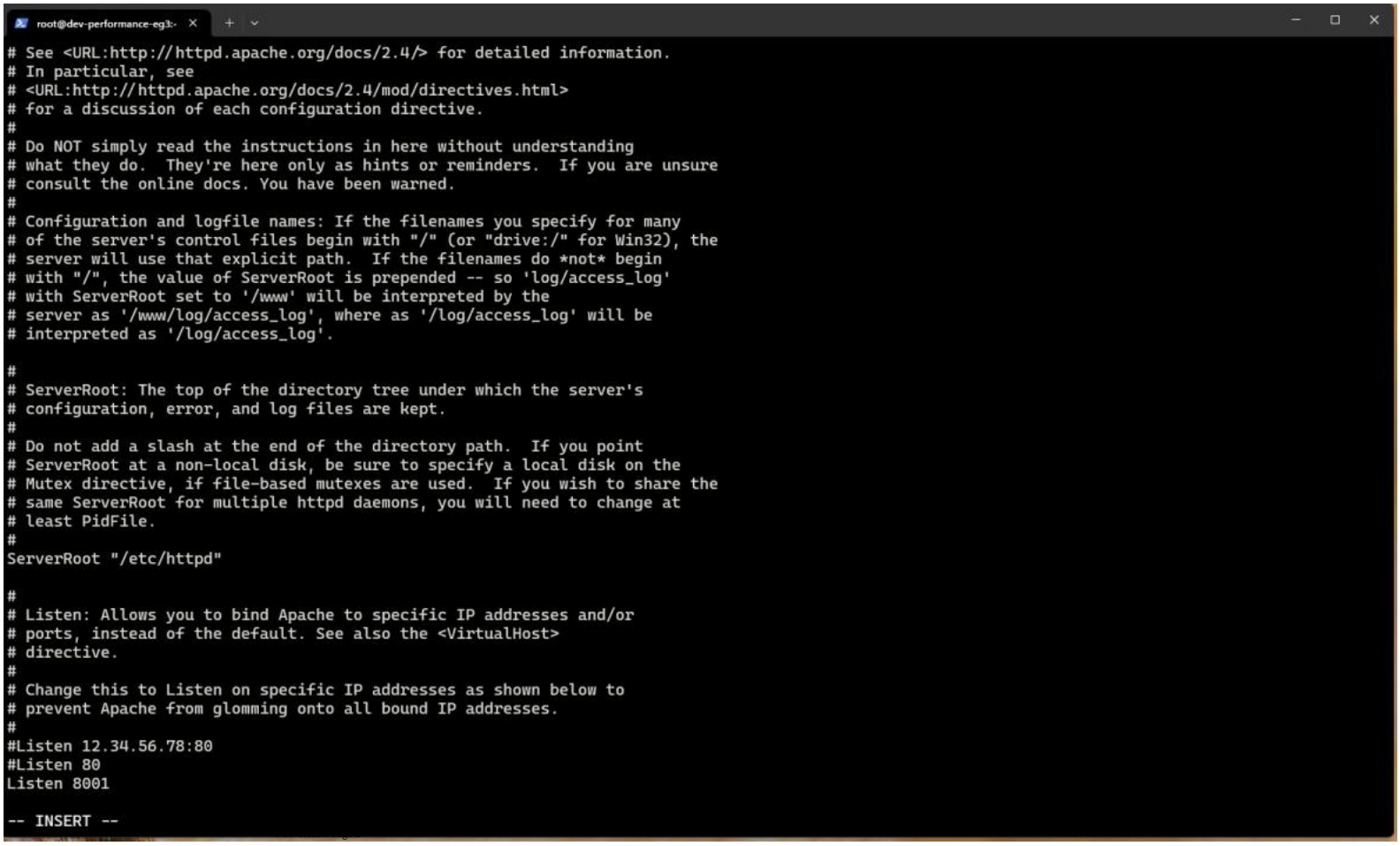
Result

Apache was successfully reconfigured to listen on port 8001 while maintaining system security controls. The service started cleanly, passed all validation checks, and served web content as expected on the new port.

Configuration Explanation

This screen shows the Apache HTTP Server configuration file being edited on a Linux system. The httpd.conf file is opened in a terminal text editor, and the Listen directive is being modified to change the port on which Apache accepts incoming connections. By default, Apache listens on port 80; in this configuration, the service is updated to listen on an alternate port (8001).

Changing the listening port allows the web server to run alongside other services or comply with environment-specific requirements without conflicting with the default HTTP port. This change requires corresponding updates to system security settings, such as firewall rules and SELinux port labeling, to allow traffic on the new port. After saving the configuration, the Apache service must be restarted for the new settings to take effect.

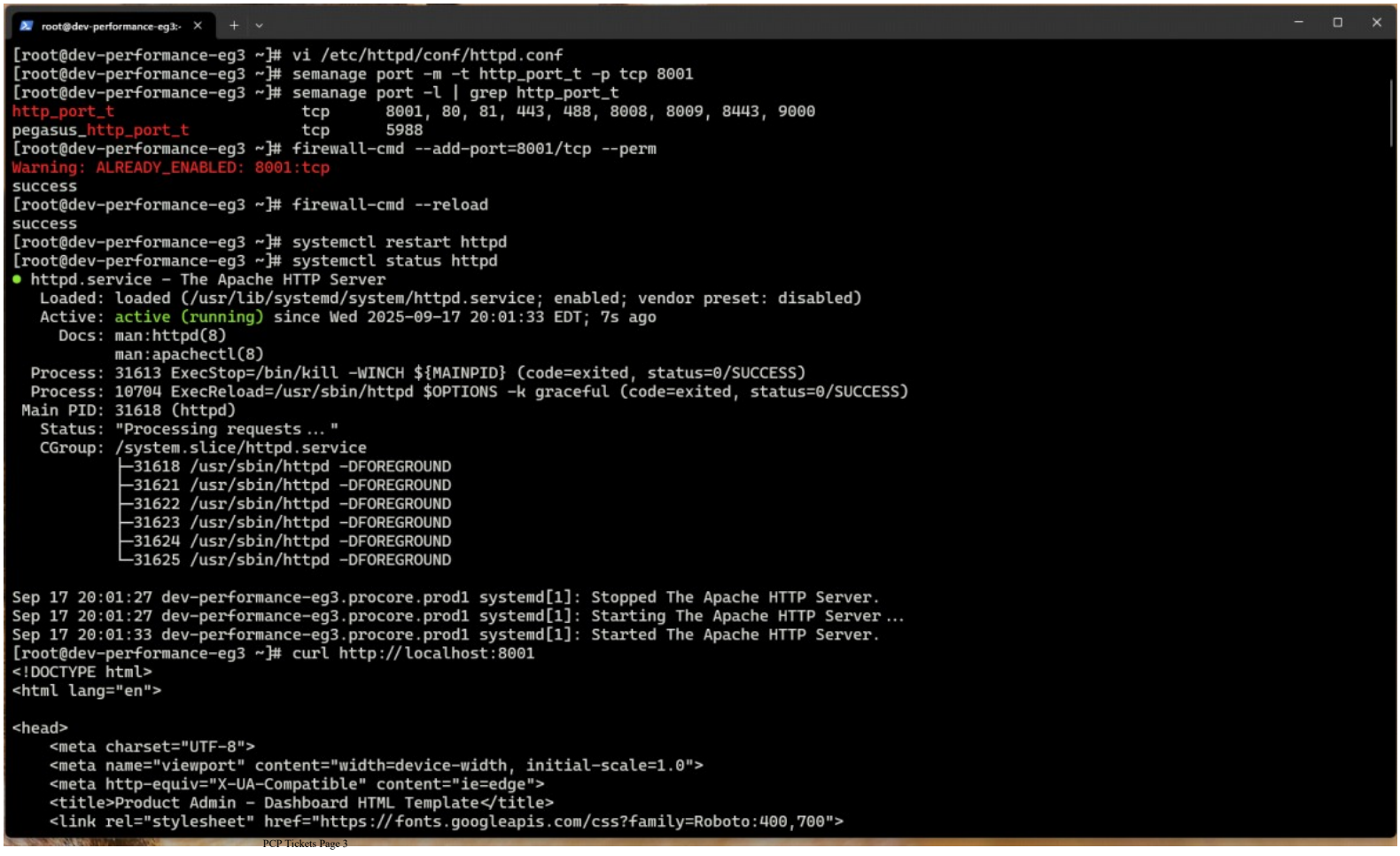


Apache Port Configuration and Verification

This screen shows the process of configuring the Apache HTTP Server to listen on a non-default port (8001) and validating that the service is running correctly. The Apache configuration file (/etc/httpd/conf/httpd.conf) is edited to update the Listen directive, allowing Apache to bind to the new port.

SELinux is then configured to permit Apache to use port 8001 by associating it with the http_port_t context using semanage port. The output confirms that the port is already properly labeled, ensuring SELinux enforcement does not block the service. The system firewall is also updated to allow inbound traffic on TCP port 8001, and the firewall configuration is reloaded to apply the change.

After applying these security updates, the Apache service is restarted to load the new configuration. The service status is checked to confirm that httpd is active and running without errors. Finally, local access is verified using curl http://localhost:8001, which returns the expected HTML output, confirming that Apache is successfully serving content on the new port.



Summary

Apache was reconfigured to listen on a non-default port (8001) by updating the HTTP server configuration. SELinux was validated and configured to allow Apache to bind to the new port, and firewall rules were applied to permit inbound traffic. The Apache service was restarted and verified as running successfully. Connectivity was confirmed by accessing the web service locally using curl, validating that Apache is serving content correctly on the new port.