Apache - PASE Authentication, Authorization and Access Control

Applies To:

[Zend Core V2.x]
[IBM System i]

Overview

This is the main Apache Server Configuration file, It contains the configuration directives that give the server its instructions (powered by Apache)..

The PASE apache server for IBM System i includes a rich collection of enhancements and features for a secure connection and a rich set of security features and services that pertain to the goals of authentication, authorization, integrity, confidentiality, and auditing.

- **Authentication** is the process by which you verify a user's identity through some sort of credentials. (userid/password, DCM, Voice recognition, fingerprinting etc.).
- **Authorization** is any process by which someone is allowed to be where they want to go, or to have information that they want to have.
- **Access Control** is a set of policies that define who can access your data, and resources, what kind of authority granted and actions allowed to perform.
- **htpasswd** is used to create and update the flat-files used to store usernames and password for basic authentication of HTTP users. If htpasswd cannot access a file, such as not being able to write to the output file or not being able to read the file in order to update it, it returns an error status and makes no changes.

Note

PASE based Apache server is supported via the IBM Web Administration for i5/OS. It allows users to list, start, stop PASE based Apache server instances and edit their configuration files via IBM Web Administration for i5/OS.

Instructions

Protecting PASE apache content with basic authentication

There are two configuration steps which you must complete in order to protect a resource using basic apache PASE authentication, grouping alike users depending on what you are trying to do.

1. Create a password file From an i5/OS command line:
   - CALL QP2TERM run the following commands from the terminal shell
   - cd */usr/local/zend/apache2/bin* the command htpasswd located in the bin directory.
   - htpasswd

     -c /password_file userid -- (created in the root directory) Choose your directory for the password file
   - htpasswd -b /password_file userid userpasswrd -- Add user and passwords to the password file
2. Set the PASE apache configuration to use this password file:
   - WRKLNK */usr/local/zend/apache2/conf*
   - Identify the PASE apache directive

```
<Directory "/www/zendcore/htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Order deny,allow
#- Deny from all
#- Allow from 127.0.0.1
Allow from all
#-----add the information created in step one ----------
AuthType basic
AuthName "Signon welcome message"
AuthUserFile /mydirectory/mypasswordfile
Require valid-user
#-----added ----------
</Directory>
```

3.Optionally, create a Group File From an i5 command line:

- EDTF STMF('*/mydir/mygroupfile*')
- File structure - GroupName: userid1 userid2 userid3

Note

The following configuration setup works for PASE apache direct requests.(reverse proxy not used)

Result

You have information on your web site that is sensitive or intended for only a small group of people, the techniques in this article will help you make sure that only users with proper credentials will have access to the information.

Excerpt: Apache - PASE Authentication, Authorization and Access Control

Original Post Date: 2009-10-23 14:09:15

External Links: http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp

http://www-03.ibm.com/servers/enable/site/porting/iseries/pase/misc.html

Alternative Description:

Apache - PASE Authentication, Authorization and Access Control