7ef8bd8d60

rconfig / www / ldap / authenticate.php / <> Jump to

rconfig fixed ldap_host NOT NULL for sql install file

History

1 contributor

65 lines (52 sloc) | 1.66 KB

```php
<?php
error_reporting(E_ALL);
ini_set('display_errors', 1);

function authenticate($user, $password) {
        if(empty($user) || empty($password)) return false;

        // active directory server
        $ldap_host = "192.168.1.224";

        // active directory DN (base location of ldap search)
        $ldap_dn = "OU=corp,DC=rconfig,DC=local";

        // active directory user group name
        $ldap_user_group = "rconfigusers";

        // active directory manager group name
        $ldap_manager_group = "rconfigusers";

        // domain, for purposes of constructing $user
        $ldap_usr_dom = '@rconfig.local';

        // connect to active directory
        $ldap = ldap_connect($ldap_host);

        // configure ldap params
        ldap_set_option($ldap,LDAP_OPT_PROTOCOL_VERSION,3);
        ldap_set_option($ldap,LDAP_OPT_REFERRALS,0);

        // verify user and password
        if($bind = @ldap_bind($ldap, $user.$ldap_usr_dom, $password)) {
                // valid
                // check presence in groups
                $filter = "(sAMAccountName=".$user.")";
                $attr = array("memberof");
                $result = ldap_search($ldap, $ldap_dn, $filter, $attr) or exit("Unable to search LDAP server");
                $entries = ldap_get_entries($ldap, $result);
                ldap_unbind($ldap);

                // check groups
                $access = 0;
                foreach($entries[0]['memberof'] as $grps) {
                        // is manager, break loop
                        if(strpos($grps, $ldap_manager_group)) { $access = 2; break; }

                        // is user
                        if(strpos($grps, $ldap_user_group)) $access = 1;
                }

                if($access != 0) {
                        // establish session variables
                        $_SESSION['user'] = $user;
                        $_SESSION['access'] = $access;
                        return true;
                } else {
                        // user has no rights
                        return false;
                }
        } else {
                // invalid name or password
                return false;
        }
}
?>
```