Contents

Extension/LDAPAuthentication

The content format pdf is not supported by the content model wikitext.

Return to Main Page.

View source for Manual:Extension/LDAPAuthentication/LDAP

You do not have permission to edit this page, for the following reason:

The action you have requested is limited to users in one of the groups: Administrators, Bureaucrats, Editors, Reviewers, Book_publisher.

You can view and copy the source of this page.

/etc/ldapprovider.json ==ldapprovider.json== <syntaxhighlight lang="json"> { "DOMAIN OF CUSTOMER": { "connection": { "server": "", "user": "", "pass": "", "basedn": "", "userbasedn": "", "groupbasedn": "", "searchattribute": "samaccountname", "usernameattribute": "samaccountname", "realnameattribute": "displayname", "emailattribute": "mail", "grouprequest": "MediaWiki\\Extension\\LDAPProvider\\UserGroupsRequest\\GroupMember::factory", "nestedgroups": true }, "authorization": { "rules": { "groups": { "required": [""] } } }, "userinfo": { "attributes-map": { "email": "mail", "realname": "displayname", } }, "groupsync": { "mechanism": "allgroups" } } } </syntaxhighlight> ==090-LDAP.php== <syntaxhighlight lang="php"> wfLoadExtensions(['Auth_remoteuser',// only needed if SingleSignOn is used 'LDAPProvider', 'Manual:Extension/LDAPAuthentication2', 'LDAPAuthorization', 'LDAPGroups', 'LDAPUserInfo', 'PluggableAuth']); $LDAPProviderDomainConfigs = "/etc/ldapprovider.json"; $Manual:Extension/LDAPAuthentication2AllowLocalLogin = false; $Manual:Extension/LDAPAuthentication2UsernameNormalizer = 'strtolower'; $LDAPProviderCacheTime = 300; $LDAPProviderCacheType = CACHE_MEMCACHED; // or CACHE_NONE if no memcached is installed $LDAPAuthorizationAutoAuthRemoteUserStringParser = 'username-at-domain'; // remove if your $_SERVER['REMOTE_USER'] is like "domain\user". If you have to remove this, follow step 2 $bsgPermissionConfig ['autocreateaccount'] = ['type' => 'global', "roles" => ['autocreateaccount']]; $wgAuthRemoteuserUserName = function() { global $wgDBname; $user = ''; if(isset($_SERVER['REMOTE_USER'])) { $user = $_SERVER['REMOTE_USER']; } //Bypass fot Parsoid / PhantomJS calls if(isset($_SERVER['REMOTE_ADDR']) && substr($_SERVER['REMOTE_ADDR'], 0, 4) == '127.') { if(empty($user)) { // check the 304f3058RemoteToken name of your cookies in your browser! $user = $_COOKIE [$wgDBname.'304f3058RemoteToken'] . '@DOMAIN OF CUSTOMER'; // Step 2: change this to $user = 'DOMAIN OF CUSTOMER\\' . $_COOKIE[$wgDBname.'304f3058RemoteToken']; } } return $user; }; </syntaxhighlight> {{Hinweis|This part "304f3058" of the cookie will change on some reasons. It should not, but we've seen it. So check with the cookies in your browser. $wgDBname is set in your LocalSettings.php }}

Template used on this page:

- Template:Hinweis (view source)

Return to Manual:Extension/LDAPAuthentication/LDAP.

View source for Manual:Extension/LDAPAuthentication/SSO

You do not have permission to edit this page, for the following reason:

The action you have requested is limited to users in one of the groups: Administrators, Bureaucrats, Editors, Reviewers, Book_publisher.

You can view and copy the source of this page.

{{DISPLAYTITLE:Install Single Sign on with Kerberos at CentOS 7.5.1408}} __TOC__ ==About this manual== In this manual we will use certain placeholders. Replace them due to the following steps analogical to your system environment. *<code>example.local</code> = your domain name *<code>webserver.example.local</code> = FQDN of your bluespice webserver *<code>dc.example.local</code> = FQDN of your domain controller ==Preparation== Please make sure that you configured a working "A" record at your DNS server for <code>webserver.example.local</code> '"and"' (really necessary!) an reverse DNS record (PTR). Please make also sure that the system clocks do not differ more than 5 minutes. ==Needed users in the Active Directory== You need to create the following users in your Active Directory *One user for your Kerberos authentication (We will call it "KerberosProxy" at this manual) *One user for your BlueSpice AD proxy user (We will call it "LdapProxy" at this manual) Please create these users and configure the passwords to "never expire". <bs:uepagebreak /> ==Create a keytab file== Create a keytab file at your domain controller using this command (works on Windows >= 2018 R2): <source lang="bash"> $ ktpass -princ HTTP/webserver.example.local@EXAMPLE.LOCAL -mapuser KerberosProxy@EXAMPLE.LOCAL -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -pass <password-of-KerberosProxy> -out bluespice.keytab </source> Move this file to your BlueSpice server (folder <code>/etc</code>). ==Install required packages on CentOS== Install all packages you need for Kerberos: <source lang="bash"> $ yum install krb5-workstation mod_auth_kerb </source> ==Create Kerberos configuration== Create a backup of <code>/etc/krb5.conf</code> and clear the file content. Insert this new content: <source lang="bash"> [libdefaults] default_realm = EXAMPLE.LOCAL [realms] EXAMPLE.LOCAL = { kdc = dc.example.local admin_server = dc.example.local } [domain_realm] example.local = EXAMPLE.LOCAL .example.local = EXAMPLE.LOCAL </source> ==Test authentication with your Keytab-file== Now you can test your authentication with the keytab file which was created before: <source lang="bash"> $ kinit -VV -k -t /etc/bluespice.keytab HTTP/webserver.example.local </source> If everything is configured correctly you should get a success message: <source lang="bash">Authenticated to Kerberos v5</source> <bs:uepagebreak /> ==Secure your BlueSpice webroot with Kerberos== Now you have to secure the BlueSpice DocumentRoot with. Open your VirtualHost config and insert the following: <source lang="bash"> <VirtualHost *:443> ... <Directory /path/to/DocumentRoot> AuthType Kerberos KrbAuthRealms EXAMPLE.LOCAL KrbServiceName HTTP/webserver.example.local@EXAMPLE.LOCAL Krb5Keytab "/etc/bluespice.keytab" KrbMethodNegotiate on KrbMethodK5Passwd on Require valid-user </Directory> ... </VirtualHost> </source> Restart your apache2 webserver. ==Testing== Create a file <code>test.php</code> at the DocumentRoot of BlueSpice and insert this code: <source lang="php"> <?php echo $_SERVER ['REMOTE_USER']; </source> If everyting works fine you should be able to open <code>test.php</code> with a webbrowser (not Firefox!) without getting an authentication window and you can see your windows user name at the <code>test.php</code>. Now delete <code>test.php</code>. ==User permission to autocreate account== Make sure that the wiki user group <code>*</code> has the <code>autocreateaccount</code> permission in the PermissionManager of BlueSpice. ==PHP-extension for ldap== Make sure that <code>php-ldap</code> is installed and loaded at your apache2 server.

Return to Manual:Extension/LDAPAuthentication/SSO.