NAME

autofs_ldap_auth.conf − autofs LDAP authentication configuration

DESCRIPTION

LDAP authenticated binds, TLS encrypted connections and certification may be used by setting appropriate values in the autofs authentication configuration file and configuring the LDAP client with appropriate settings. The default location of this file is **/etc/autofs_ldap_auth.conf**. If this file exists it will be used to establish whether TLS or authentication should be used.

An example of this file is:

```
<?xml version="1.0" ?>
<autofs_ldap_sasl_conf
        usetls="yes"
        tlsrequired="no"
        authrequired="no"
        authtype="DIGEST-MD5"
        user="xyz"
        secret="abc"
/>
```

If TLS encryption is to be used the location of the Certificate Authority certificate must be set within the LDAP client configuration in order to validate the server certificate. If, in addition, a certified connection is to be used then the client certificate and private key file locations must also be configured within the LDAP client.

OPTIONS

This files contains a single XML element, as shown in the example above, with several attributes.

The possible attributes are:

usetls="yes"|"no"
Determines whether an encrypted connection to the ldap server should be attempted.

tlsrequired="yes"|"no"
This flag tells whether the ldap connection must be encrypted. If set to "yes", the automounter will fail to start if an encrypted connection cannot be established.

authrequired="yes"|"no"|"autodetect"|"simple"
This option tells whether an authenticated connection to the ldap server is required in order to perform ldap queries. If the flag is set to yes, only sasl authenticated connections will be allowed. If it is set to no then authentication is not needed for ldap server connections. If it is set to autodetect then the ldap server will be queried to establish a suitable sasl authentication mechanism. If no suitable mechanism can be found, connections to the ldap server are made without authentication. Finally, if it is set to simple, then simple authentication will be used instead of SASL.

authtype="GSSAPI"|"LOGIN"|"PLAIN"|"ANONYMOUS"|"DIGEST-MD5|EXTERNAL"
This attribute can be used to specify a preferred authentication mechanism. In normal operations, the automounter will attempt to authenticate to the ldap server using the list of supported-SASLmechanisms obtained from the directory server. Explicitly setting the authtype will bypass this selection and only try the mechanism specified. The EXTERNAL mechanism may be used to authenticate using a client certificate and requires that authrequired set to "yes" if using SSL or usetls, tlsrequired and authrequired all set to "yes" if using TLS, in addition to authtype being set to EXTERNAL.

If using authtype EXTERNAL two additional configuration entries are required:

external_cert="<client certificate path>"

This specifies the path of the file containing the client certificate.

external_key="<client certificate key path>"

This specifies the path of the file containing the client certificate key.

These two configuration entries are mandatory when using the EXTERNAL method as the HOME environment variable cannot be assumed to be set or, if it is, to be set to the location we expect.

user="<username>"
This attribute holds the authentication identity used by authentication mechanisms that require it. Legal values for this attribute include any printable characters that can be used by the selected authentication mechanism.

secret="<password>"
This attribute holds the secret used by authentication mechanisms that require it. Legal values for this attribute include any printable characters that can be used by the selected authentication mechanism.

encoded_secret="<base64 encoded password>"
This attribute holds the base64 encoded secret used by authentication mechanisms that require it. If this entry is present as well as the secret entry this value will take precedence.

clientprinc="<GSSAPI client principal>"
When using GSSAPI authentication, this attribute is consulted to determine the principal name to use when authenticating to the directory server. By default, this will be set to "autofsclient/<fqdn>@<REALM>.

credentialcache="<external credential cache path>"
When using GSSAPI authentication, this attribute can be used to specify an externally configured credential cache that is used during authentication. By default, autofs will set-up a memory based credential cache.

SEE ALSO

auto.master(5), **autofs.conf**(5),

AUTHOR

This manual page was written by Ian Kent <raven@themaw.net>.