Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'authselect-migration.7'

$ man authselect-migration.7

AUTHSELECT-MIGRATIO(7) AUTHSELECT-MIGRATIO(7)

NAME

authselect-migration - A guide how to migrate from authconfig to authselect.

DESCRIPTION

This manual page explains the main differences between authconfig, the previous tool to configure system authentication and identity sources, and authselect which replaces it. It also explains what actions need to be done in order to migrate from authconfig to authselect.

MAIN DIFFERENCES

Authselect takes a completely different approach to system configuration than the previous tool authconfig.

Authconfig tries its best to keep users?s manual changes to the files it generates. It generates not only PAM configuration files and nsswitch.conf (to setup authentication modules and identity sources) but it also generates simple configuration files for several services such as LDAP and Kerberos.

Authselect does no such things. It does not generate any configuration files beside PAM and nsswitch.conf and it strictly prohibits any manual changes to generated configuration. It provides a set of files called profiles. Each profile describes how the resulting configuration should look like and it can be slightly modified by enabling or disabling certain optional features. If a need arises for a different profile than what authselect ships, the administrator has an option to create a whole new profile and use it with authselect. See authselect-profiles(5) to learn more about profiles.

This may seem like a big disadvantage but the truth is the opposite. Authconfig is a very old tool and the applications providing required services have changed rapidly over the years. Typically, there is no longer a need to have multiple authentication modules in PAM and nsswitch.conf, because the vast majority of use-cases is covered by SSSD. Therefore there is no need to add or remove them specifically. There are also better tools to generate configuration for system daemons that can help you automate the process of joining to a remote domain such as realm. In addition, the shipped profiles give us comprehensive and deterministic system configuration that can be fully tested and is much less error prone. It is also much easier to distribute such configuration across many systems.

Probably the most controversial change is that authselect only ships profiles for sssd and winbind providers. Those two providers cover all modern use cases from providing local users and legacy LDAP domain to complex configurations with IPA or Active Directory servers. The profiles no longer contain support for nss-pam-ldapd and users are encouraged to switch to sssd.

JOINING REMOTE DOMAINS

You can use either ipa-client-install or realm to join an IPA domain and realm to join an Active Directory domain. These tools will make sure that the correct authselect profile is selected and all daemons and services are properly configured.

CONVERTING YOUR SCRIPTS

If you use ipa-client-install or realm to join a domain, you can just remove any authconfig call in your scripts. If this is not an option, you need to replace each authconfig call with its equivalent authselect call to select a correct profile with desired features. Then you also need to write configuration file for required services.

Table 1. Relation of authconfig options to authselect profiles

Authconfig options	Authselect profile
--enableldap --enableldapauth	sssd
--enablesssd --enablesssdauth	sssd
--enablekrb5	sssd
--enablewinbind --enablewinbindauth	winbind
--enablenis	none

Table 2. Relation of authconfig options to authselect profile features

Authconfig options	Authselect profile feature

```
?--enablesmartcard   ? with-smartcard             ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enablefingerprint ? with-fingerprint           ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enablemkhomedir   ? with-mkhomedir             ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enablefaillock    ? with-faillock              ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enablepamaccess   ? with-pamaccess             ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enablewinbindkrb5 ? with-krb5                  ?
??????????????????????????????????????????????????
?                    ?                            ?
?--enableshadow      ? none                       ?
??????????????????????????????????????????????????
?                    ?                            ?
?--passalgo          ? none                       ?
??????????????????????????????????????????????????
```

Note

Authconfig options --enableshadow and --passalgo=sha512 were often used to make sure that passwords are stored in /etc/shadow using sha512 algorithm. The authselect profiles now use the sha512 hashing method and it cannot be changed through an option (only by creating a custom profile). You can just omit these options.

Examples.

```
    authconfig --enableldap --enableldapauth --enablefaillock --updateall
    authselect select sssd with-faillock
    authconfig --enablesssd --enablesssdauth --enablesmartcard --smartcardmodule=sssd --updateall
```

```
authselect select sssd with-smartcard

authconfig --enablepamaccess --updateall

authselect select sssd with-pamaccess

authconfig --enablewinbind --enablewinbindauth --winbindjoin=Administrator --updateall

realm join -U Administrator --client-software=winbind WINBINDDOMAIN
```

CONFIGURATION FILES

This section contains snippets for minimal configuration of various services.

LDAP

Even if LDAP is not directly used through pam_ldap and nss_ldap, it is still useful to configure ldap.conf to configure openldap-libs and indirectly, e.g. LDAP tools such as ldapsearch.

/etc/openldap/ldap.conf.

```
# Set the default base dn
BASE   dc=example,dc=com
# Set the default LDAP server
URI    ldap://ldap.example.com ldap://ldap-master.example.com:666
```

KERBEROS

If you use Kerberos, the default Kerberos realm should be configured in order for krb5-libs and therefore tools such as kinit to work out of the box.

/etc/krb5.conf.

```
[libdefaults]
 default_realm = MYREALM
[realms]
 MYREALM = {
  kdc = kdc.myrealm.org
 }
[domain_realm]
 myrealm.org = MYREALM
 .myrealm.org = MYREALM
```

SSSD

Authselect encourages users to use SSSD wherever possible. There are many configuration options, see sssd.conf(5). This is a minimal configuration that creates one LDAP domain called default. The LDAP server is auto-discovered through DNS lookups.

/etc/sssd/sssd.conf.

```
[sssd]
config_file_version = 2
domains = default
[domain/default]
id_provider = ldap
ldap_uri = _srv_
dns_discovery_domain = myrealm
```

And here is a configuration snippet for the same domain but now the authentication is done over Kerberos. The KDC server is auto-discovered through DNS lookups.

/etc/sssd/sssd.conf.

```
[sssd]
config_file_version = 2
domains = default
[domain/default]
id_provider = ldap
auth_provider = krb5
ldap_uri = _srv_
krb5_server = _srv_
krb5_realm = MYREALM
dns_discovery_domain = myrealm
```

If you want to configure SSSD for an IPA or Active Directory domain, use the realm tool. This will perform an initial setup which involves creating a Kerberos keytab and generating basic SSSD configuration. You can then tune it up by modifying /etc/sssd/sssd.conf.

WINBIND

If you want to configure the machine to use Winbind, use realm. This will perform an initial setup which involves creating a Kerberos keytab and running adcli to join the domain. It also makes changes to smb.conf. You can then tune it up by modifying /etc/samba/smb.conf.

NIS

There are several places that needs to be configured in order to make NIS authentication work. First, you need to set NIS domain and optionally also NIS server in /etc/yp.conf.

/etc/yp.conf.

```
domain mydomain broadcast
# or
# domain mydomain server myserver
```

NIS domain must be also set in system network configuration.

/etc/sysconfig/network.

```
NISDOMAIN=mydomain
```

Now, you can set the domain name with command line so there is no need to reboot your system. Additionaly, it may be necessary to enable NIS in selinux.

```
$ domainname mydomain
$ setsebool -P allow_ypbind 1
```

PASSWORD QUALITY

Authselect enables pam_pwquality module to enforce password quality restrictions. This module is enabled only for local users. Remote users should use the password policy that is enforced by the respective remote server.

The pam_pwquality module can be configured in /etc/security/pwquality.conf. See pam_pwquality(8) to see its configuration options and defaults.

STARTING SERVICES

Depending on your configuration, you need to start required services manually with systemd.

? SSSD

```
systemctl enable sssd.service ; systemctl start sssd.service
```

? Winbind

```
systemctl enable winbind.service ; systemctl start winbind.service
```

? NIS

```
systemctl enable rpcbind.service ; systemctl start rpcbind.service

systemctl enable ypbind.service ; systemctl start ypbind.service
```

? If mkhomedir feature is enabled

```
systemctl enable oddjobd.service ; systemctl start oddjobd.service
```

AUTHCONFIG TOOLS

Authconfig shipped a tool called cacertdir_rehash. If you depend on this tool, please switch to native openssl command: openssl rehash <directory> that serves the same purpose.

SEE ALSO

authselect(8), authselect-profiles(5), realm(8), ipa-client-install(1), sssd.conf(5), smb.conf(5), ldap.conf(5), krb5.conf(5)