Red Hat Enterprise Linux 8

Configuring authentication on a Red Hat Enterprise Linux host

Using authselect

Last Updated: 2019-05-07

Red Hat Enterprise Linux 8 Configuring authentication on a Red Hat Enterprise Linux host

Using authselect

Legal Notice

Abstract

This documentation collection provides instructions on how to plan and configure authentication on a Red Hat Enterprise Linux 8 host.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the **Add Feedback** pop-up that appears below the highlighted text, and follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
    1. Go to the Bugzilla website.
    2. As the Component, use **Documentation**.
    3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
    4. Click **Submit Bug**.

CHAPTER 1. USING AUTHSELECT

1.1. EXPLAINING AUTHSELECT

Authselect is a utility that simplifies the configuration of user authentication on a Red Hat Enterprise Linux host. **Authselect** offers two ready-made profiles that can be universally used with all modern identity management systems:

- the **sssd** profile
- the **winbind** profile

For legacy compatibility reasons, the **nis** profile is also available.

Red Hat recommends using **authselect** in semi-centralized identity management environments, for example if your company utilizes the LDAP, winbind or nis databases to authenticate users to use services in your domain.

WARNING

Do not use **authselect** if your host is part of Red Hat Enterprise Linux Identity Management or Active Directory. The **ipa-client-install** command, called when joining your host to a Red Hat Identity Management domain, takes full care of configuring authentication on your host. Similarly the **realm join** command, called when joining your host to an Active Directory domain, takes full care of configuring authentication on your host.

The **authconfig** utility, used in previous Red Hat Enterprise Linux versions, created and modified many different configuration files, making troubleshooting a difficult task. **Authselect** makes testing and troubleshooting easy because it only modifies files in these directories:

- **/etc/nsswitch.conf**
- **/etc/pam.d/*** files
- **/etc/dconf/db/distro.d/*** files

The Name Service Switch (NSS) configuration file, **/etc/nsswitch.conf**, is used by the GNU C Library and certain other applications to determine the sources from which to obtain name-service information in a range of categories, and in what order. Each category of information is identified by a database name.

Linux-PAM (Pluggable Authentication Modules) is a system of modules that handle the authentication tasks of applications (services) on the system. The nature of the authentication is dynamically configurable: the system administrator can choose how individual service-providing applications will authenticate users. This dynamic configuration is set by the contents of the configuration files in the **/etc/pam.d/** directory, which list the PAMs that will do the authentication tasks required by this service, and the appropriate behavior of the PAM-API in the event that individual PAMs fail.

Once an **authselect** profile is selected for a given host, the profile will be applied to every user logging into the host.

1.2. CHOOSING AN AUTHSELECT PROFILE

As a system administrator, you can select a profile for the **authselect** utility for a specific host. The profile will be applied to every user logging into the host.

Procedure

1. Select the **authselect** profile that is appropriate for your authentication provider. For example, for logging into the network of a company that uses LDAP, choose **sssd**. Run the command as root:

```
# authselect select sssd
```

2. Optionally, review the contents of the **/etc/nsswitch.conf** file:

```
passwd:     sss files
group:      sss files
netgroup:   sss files
automount:  sss files
services:   sss files
...
```

The content of the **/etc/nsswitch.conf** file shows that selecting the **sssd** profile means that the system first uses **sssd** if information concerning one of the first five items is requested. Only if the requested information is not found in the **sssd** cache and on the server providing authentication, or if **sssd** is not running, the system looks at the local files, that is **/etc/***.

For example, if information is requested about a user id, the user id is first searched in the **sssd** cache. If it is not found there, the **/etc/passwd** file is consulted. Analogically, if a user's group affiliation is requested, it is first searched in the **sssd** cache and only if not found there, the **/etc/group** file is consulted.

In practice, the local **files** database does not normally get consulted at all. The only exception is the case of the **root** user, which is never handled by **sssd** but by **files**.

3. Optionally, review the contents of the **/etc/pam.d/system-auth** file:

```
# Generated by authselect on Tue Sep 11 22:59:06 2018
# Do not modify this file manually.

auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]    pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]    pam_localuser.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient    pam_sss.so forward_pass
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
...
```

Among other things, the **/etc/pam.d/system-auth** file contains information about:

- user password lockout condition
- the possibility to authenticate with a smart card
- the possibility to authenticate with fingerprints
  You can modify the default profile settings by adding the following options to the **authselect select sssd** or **authselect select winbind** command, for example:
  - **with-faillock**
  - **with-smartcard**
  - **with-fingerprint**

To see the full list of available options, see Section 1.5, "Converting your scripts from authconfig to authselect" or the authselect-migration(7) man page.

NOTE

Make sure that the configuration files that are relevant for your profile are configured properly before finishing the **authselect** select procedure. For example, if the **sssd** daemon is not configured correctly and active, running **authselect select** results in only local users being able to authenticate, using pam_unix.

If adjusting a ready-made profile by adding one of the **authselect select** command-line options described above is not enough for your use case, you can:

- modify a ready-made profile by changing the **/etc/authselect/user-nsswitch.conf** file. For details, see Section 1.3, "Modifying a ready-made authselect profile" .
- create your own custom profile. For details, see Section 1.4, "Creating and deploying your own custom authselect profile".

1.3. MODIFYING A READY-MADE AUTHSELECT PROFILE

As a system administrator, you can modify one of the default profiles, the **sssd**, **winbind**, or the **nis** profile, to suit your needs. You can modify any of the items in the **/etc/authselect/user-nsswitch.conf** file with the exception of:

- passwd
- group
- netgroup
- automount
- services

Running **authselect select profile_name** afterwards will result in permissible changes to the profile being transferred from **/etc/authselect/user-nsswitch.conf** to the **/etc/nsswitch.conf** file but unacceptable changes being overwritten by the default profile configuration.

IMPORTANT

Do not modify the **/etc/nsswitch.conf** file directly.

Procedure

1. Select an **authselect** profile, for example:

```
# authselect select sssd
```

2. Edit the **/etc/authselect/user-nsswitch.conf** file.

3. Apply the changes from the **/etc/authselect/user-nsswitch.conf** file:

```
# authselect apply-changes
```

4. Optionally, review the **/etc/nsswitch.conf** file to verify that the changes from **/etc/authselect/user-nsswitch.conf** have been propagated there.

1.4. CREATING AND DEPLOYING YOUR OWN CUSTOM AUTHSELECT PROFILE

As a system administrator, you can create and deploy a custom profile by customizing one of the default profiles, the **sssd**, **winbind**, or the **nis** profile. This is particularly useful if Section 1.3, "Modifying a ready-made authselect profile" is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host.

Procedure

1. Create your custom profile by using the **authselect create-profile** command. For example, to create a custom profile called **user-profile** based on the ready-made **sssd** profile but one in which you can configure the items in the **/etc/nsswitch.conf** file yourself:

```
# authselect create-profile user-profile -b sssd --symlink-meta --symlink-pam
New profile was created at /etc/authselect/custom/user-profile
```

   Including the **--symlink-pam** option in the command means that PAM templates will be symbolic links to the origin profile files instead of their copy; including the **--symlink-meta** option means that meta files, such as README and REQUIREMENTS will be symbolic links to the origin profile files instead of their copy. This ensures that all future updates to the PAM templates and meta files in the original profile will be reflected in your custom profile, too.

   The command has created a copy of the **/etc/nsswitch.conf** file in the **/etc/authselect/custom/user-profile/** directory.

2. Configure the **/etc/authselect/custom/user-profile/nsswitch.conf** file.

3. Select the custom profile by running the **authselect select** command, and adding custom/*name_of_the_profile* as a parameter. For example, to select the **user-profile** profile:

```
# authselect select custom/user-profile
```

Selecting the **user-profile** profile for your machine means that if the **sssd** profile is subsequently updated by Red Hat, you will benefit from all the updates with the exception of updates made to the **/etc/nsswitch.conf** file.

Example

The following procedure shows how to create a profile based on the **sssd** profile which only consults the local static table lookup for hostnames in the **/etc/hosts** file, not in the **dns** or **myhostname** databases.

1. Edit the **/etc/nsswitch.conf** file by editing the following line:

```
hosts:      files
```

2. Create a custom profile based on **sssd** that excludes changes to **/etc/nsswitch.conf**:

```
# authselect create-profile user-profile -b sssd --symlink-meta --symlink-pam
```

3. Select the profile:

```
# authselect select custom/user-profile
```

4. Optionally, check that selecting the custom profile has
   - created the **/etc/pam.d/system-auth** file according to the chosen **sssd** profile
   - left the configuration in the **/etc/nsswitch.conf** unchanged:

```
hosts:      files
```

NOTE

Running **authselect select sssd** would, in contrast, result in

```
hosts:      files dns myhostname
```

1.5. CONVERTING YOUR SCRIPTS FROM AUTHCONFIG TO AUTHSELECT

If you use **ipa-client-install** or **realm join** to join a domain, you can safely remove any **authconfig** call in your scripts. If this is not possible, replace each **authconfig** call with its equivalent **authselect** call. In doing that, select the correct profile and the appropriate options. In addition, edit the necessary configuration files:

- **/etc/krb5.conf**
- **/etc/sssd/sssd.conf** (for the **sssd** profile) or **/etc/samba/smb.conf** (for the **winbind** profile)

Table 1.1, "Relation of authconfig options to authselect profiles" and Table 1.2, "Authselect profile option equivalents of authconfig options" show the **authselect** equivalents of **authconfig** options.

Table 1.1. Relation of authconfig options to authselect profiles

Authconfig options	Authselect profile

--enableldap --enableldapauth	**sssd**
--enablesssd --enablesssdauth	**sssd**
--enablekrb5	**sssd**
--enablewinbind --enablewinbindauth	**winbind**
--enablenis	**nis**

Table 1.2. Authselect profile option equivalents of authconfig options

Authconfig option	Authselect profile feature
--enablesmartcard	with-smartcard
--enablefingerprint	with-fingerprint
--enableecryptfs	with-ecryptfs
--enablemkhomedir	with-mkhomedir
--enablefaillock	with-faillock
--enablepamaccess	with-pamaccess
--enablewinbindkrb5	with-krb5
--enablepamaccess	with-pamaccess

Table 1.3, "Examples of authselect commands equivalents to authconfig commands" shows example transformations of Kickstart calls to **authconfig** into Kickstart calls to **authselect**.

Table 1.3. Examples of authselect commands equivalents to authconfig commands

authconfig command	authselect equivalent
authconfig --enableldap --enableldapauth --enablefaillock --updateall	authselect select sssd with-faillock
authconfig --enablesssd --enablesssdauth --enablesmartcard --smartcardmodule=sssd --updateall	authselect select sssd with-smartcard
authconfig --enableecryptfs --enablepamaccess --updateall	authselect select sssd with-ecryptfs with-pamaccess

authconfig --enablewinbind --enablewinbindauth --winbindjoin=Administrator --updateall	realm join -U Administrator --client-software=winbind **WINBINDDOMAIN**