Products & Services ❯ Product Documentation ❯ Red Hat Enterprise Linux ❯ 7 ❯ SELinux User's and Administrator's Guide ❯ 3.3. Confined and Unconfined Users

3.3. CONFINED AND UNCONFINED USERS

Each Linux user is mapped to an SELinux user using SELinux policy. This allows Linux users to inherit the restrictions on SELinux users. This Linux user mapping is seen by running the `semanage login -l` command as root:

```
~]# semanage login -l Login Name SELinux User MLS/MCS Range Service
__default__ unconfined_u s0-s0:c0.c1023 * root unconfined_u s0-
s0:c0.c1023 * system_u system_u s0-s0:c0.c1023 *
```

In Red Hat Enterprise Linux, Linux users are mapped to the SELinux `__default__` login by default, which is mapped to the SELinux `unconfined_u` user. The following line defines the default mapping:

```
__default__ unconfined_u s0-s0:c0.c1023
```

The following procedure demonstrates how to add a new Linux user to the system and how to map that user to the SELinux `unconfined_u` user. It assumes that the root user is running unconfined, as it does by default in Red Hat Enterprise Linux:

Procedure 3.4. Mapping a New Linux User to the SELinux `unconfined_u` User

1. As root, enter the following command to create a new Linux user named `newuser`:

   ```
   ~]# useradd newuser
   ```

2. To assign a password to the Linux `newuser` user. Enter the following command as root:

   ```
   ~]# passwd newuser Changing password for user newuser. New UNIX
   password: Enter a password Retype new UNIX password: Enter the
   same password again passwd: all authentication tokens updated
   successfully.
   ```

3. Log out of your current session, and log in as the Linux `newuser` user. When you log in, the **pam_selinux** PAM module automatically maps the Linux user to an SELinux user (in this case, `unconfined_u`), and sets up the resulting SELinux context. The Linux user's shell is then launched with this context. Enter the following command to view the context of a Linux user:

   ```
   [newuser@localhost ~]$ id -Z
   unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
   ```

   Note

   If you no longer need the `newuser` user on your system, log out of the Linux `newuser`'s session, log in with your account, and run the `userdel -r newuser` command as root. It will remove `newuser` along with their home directory.

Confined and unconfined Linux users are subject to executable and writable memory checks, and are also restricted by MCS or MLS.

To list the available SELinux users, enter the following command:

```
~]$seinfo -u Users: 8 sysadm_u system_u xguest_u root guest_u staff_u
user_u unconfined_u
```

Note that the `seinfo` command is provided by the setools-console package, which is not installed by default.

If an unconfined Linux user executes an application that SELinux policy defines as one that can transition from the `unconfined_t` domain to its own confined domain, the unconfined Linux user is still subject to the restrictions of that confined domain. The security benefit of this is that, even though a Linux user is running unconfined, the application remains confined. Therefore, the exploitation of a flaw in the application can be limited by the policy.

Similarly, we can apply these checks to confined users. Each confined Linux user is restricted by a confined user domain. The SELinux policy can also define a transition from a confined user domain to its own target confined domain. In such a case, confined Linux users are subject to the restrictions of that target confined domain. The main point is that special privileges are associated with the confined users according to their role. In the table below, you can see examples of basic confined domains for Linux users in Red Hat Enterprise Linux:

Table 3.1. SELinux User Capabilities

User	Role	Domain	X Window System	su or sudo	Execute in home directory and /tmp (default)	Networking
sysadm_u	sysadm_r	sysadm_t	yes	**su** and **sudo**	yes	yes
staff_u	staff_r	staff_t	yes	only **sudo**	yes	yes
user_u	user_r	user_t	yes	no	yes	yes
guest_u	guest_r	guest_t	no	no	no	no
xguest_u	xguest_r	xguest_t	yes	no	no	Firefox only

- Linux users in the `user_t`, `guest_t`, and `xguest_t` domains can only run set user ID (setuid) applications if SELinux policy permits it (for example, passwd). These users cannot run the su and sudo setuid applications, and therefore cannot use these applications to become root.

- Linux users in the sysadm_t , staff_t , user_t , and xguest_t domains can log in using the X Window System and a terminal.
- By default, Linux users in the guest_t and xguest_t domains cannot execute applications in their home directories or the /tmp directory, preventing them from executing applications, which inherit users' permissions, in directories they have write access to. This helps prevent flawed or malicious applications from modifying users' files.
- By default, Linux users in the staff_t and user_t domains can execute applications in their home directories and /tmp . See Section 6.6, "Booleans for Users Executing Applications" (sect-Security-Enhanced_Linux-Confining_Users-Booleans_for_Users_Executing_Applications) for information about allowing and preventing users from executing applications in their home directories and /tmp .
- The only network access Linux users in the xguest_t domain have is **Firefox** connecting to web pages.

Note that system_u is a special user identity for system processes and objects. It must never be associated to a Linux user. Also, unconfined_u and root are unconfined users. For these reasons, they are not included in the aforementioned table of SELinux user capabilities.

Alongside with the already mentioned SELinux users, there are special roles, that can be mapped to those users. These roles determine what SELinux allows the user to do:

- webadm_r can only administrate SELinux types related to the Apache HTTP Server. See Section 14.2, "Types" (sect-Managing_Confined_Services-The_Apache_HTTP_Server-Types) for further information.
- dbadm_r can only administrate SELinux types related to the MariaDB database and the PostgreSQL database management system. See Section 21.2, "Types" (sect-Managing_Confined_Services-MariaDB-Types) and Section 22.2, "Types" (sect-Managing_Confined_Services-PostgreSQL-Types) for further information.
- logadm_r can only administrate SELinux types related to the syslog and auditlog processes.

- `secadm_r` can only administrate SELinux.
- `auditadm_r` can only administrate processes related to the `audit` subsystem.

To list all available roles, enter the following command:

```
~]$ seinfo -r
```

As mentioned before, the `seinfo` command is provided by the setools-console package, which is not installed by default.

3.3.1. The sudo Transition and SELinux Roles

In certain cases, confined users need to perform an administrative task that require root privileges. To do so, such a confined user has to gain a *confined administrator* SELinux role using the `sudo` command. The `sudo` command is used to give trusted users administrative access. When users precede an administrative command with `sudo`, they are prompted for their *own* password. Then, when they have been authenticated and assuming that the command is permitted, the administrative command is executed as if they were the root user.

As shown in Table 3.1, "SELinux User Capabilities" (sect-Security-Enhanced_Linux-Targeted_Policy-Confined_and_Unconfined_Users#tabl-Security-Enhanced_Linux-Confined_and_Unconfined_Users-SELinux_User_Capabilities), only the `staff_u` and `sysadm_u` SELinux confined users are permitted to use `sudo` by default. When such users execute a command with `sudo`, their role can be changed based on the rules specified in the `/etc/sudoers` configuration file or in a respective file in the `/etc/sudoers.d/` directory if such a file exists.

For more information about `sudo`, see the *Gaining Privileges* section in the Red Hat Enterprise Linux 7 System Administrator's Guide (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Gaining_Privileges.html).

Procedure 3.5. Configuring the sudo Transition

This procedure shows how to set up `sudo` to transition a newly-created *SELinux_user_u* confined user from a *default_role_t* to a *administrator_r* administrator role. To configure a confined administrator role for an already existing

SELinux user, skip the first two steps. Also, note that the following commands must be run as the root user. To better understand the placeholders in the following procedure, such as *default_role_t* or *administrator_r*, see the example in step 6.

1. Create a new SELinux user and specify the default SELinux role and a supplementary confined administrator role for this user:

   ```
   ~]# semanage user -a -r s0-s0:c0.c1023 -R "default_role_r
   administrator_r" SELinux_user_u
   ```

2. Set up the default SElinux policy context file. For example, to have the same SELinux rules as the `staff_u` SELinux user, copy the `staff_u` context file:

   ```
   ~]# cp /etc/selinux/targeted/contexts/users/staff_u /etc/selinux
   /targeted/contexts/users/SELinux_user_u
   ```

3. Map the newly-created SELinux user to an existing Linux user:

   ```
   semanage login -a -s SELinux_user_u -rs0:c0.c1023 linux_user
   ```

4. Create a new configuration file with the same name as your Linux user in the `/etc/sudoers.d/` directory and add the following string to it:

   ```
   ~]# echo "linux_user ALL=(ALL) TYPE=administrator_t
   ROLE=administrator_r /bin/sh " > /etc/sudoers.d/linux_user
   ```

5. Use the `restorecon` utility to relabel the *linux_user* home directory:

   ```
   ~]# restorecon -FR -v /home/linux_user
   ```

6. When you log in to the system as the newly-created Linux user, the user is labeled with the default SELinux role:

```
~]$ id -Z
SELinux_user_u:default_role_r:SELinux_user_t:s0:c0.c1023
```

After running `sudo` , the user's SELinux context changes to the supplementary SELinux role as specified in `/etc/sudoers.d/linux_user` . The `-i` option used with `sudo` caused that an interactive shell is executed:

```
~]$ sudo -i ~]# id -Z
SELinux_user_u:administrator_r:administrator_t:s0-s0:c0.c1023
```

For the `SELinux_user_u` user from the example specified in the first step the output looks like below:

```
~]$ id -Z confined_u:staff_r:staff_t:s0:c0.c1023 ~]$ sudo -i
~]# id -Z confined_u:webadm_r:webadm_t:s0:c0.c1023
```

In the example bellow, we will create a new SELinux user `confined_u` with default assigned role `staff_r` and with `sudo` configured to change the role of `confined_u` from `staff_r` to `webadm_r` .

```
~]# semanage user -a -r s0-s0:c0.c1023 -R "staff_r webadm_r"
confined_u ~]# cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/confined_u ~]# semanage
login -a -s confined_u -rs0:c0.c1023 linux_user ~]# restorecon
-FR -v /home/linux_user ~]# echo "linux_user ALL=(ALL)
TYPE=webadm_t ROLE=webadm_r /bin/sh " > /etc/sudoers.d/linux_user
```

When you log in to the system as the newly-created Linux user, the user is labeled with the default SELinux role:

```
~]$ id -Z confined_u:staff_r:staff_t:s0:c0.c1023 ~]$ sudo -i
~]# id -Z confined_u:webadm_r:webadm_t:s0:c0.c1023
```

3.2. Unconfined Processes (/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-targeted_policy-unconfined_processes)

4. Working with SELinux (/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-working_with_selinux)

Where did the comment section go?

Red Hat's documentation publication system recently went through an upgrade to enable speedier, more mobile-friendly content. We decided to re-evaluate our commenting platform to ensure that it meets your expectations and serves as an optimal feedback mechanism. During this redesign, we invite your input on providing feedback on Red Hat documentation via the discussion platform (/node/add/discussion?field_tags[]=docs-feedback&field_product[]=red_hat_enterprise_linux).