NAME

sysusers.d − Declarative allocation of system users and groups

SYNOPSIS

/etc/sysusers.d/*.conf

/run/sysusers.d/*.conf

/usr/lib/sysusers.d/*.conf

DESCRIPTION

systemd−sysusers uses the files from sysusers.d directory to create system users and groups and to add users to groups, at package installation or boot time. This tool may be used to allocate system users and groups only, it is not useful for creating non−system (i.e. regular, "human") users and groups, as it accesses /etc/passwd and /etc/group directly, bypassing any more complex user databases, for example any database involving NIS or LDAP.

CONFIGURATION DIRECTORIES AND PRECEDENCE

Each configuration file shall be named in the style of *package*.conf or *package−part*.conf. The second variant should be used when it is desirable to make it easy to override just this part of configuration.

Files in /etc/sysusers.d override files with the same name in /usr/lib/sysusers.d and /run/sysusers.d. Files in /run/sysusers.d override files with the same name in /usr/lib/sysusers.d. Packages should install their configuration files in /usr/lib/sysusers.d. Files in /etc/sysusers.d are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same path, the entry in the file with the lexicographically earliest name will be applied. All later entries for the same user and group names will be logged as warnings.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to /dev/null in /etc/sysusers.d/ bearing the same filename.

CONFIGURATION FILE FORMAT

The file format is one line per user or group containing name, ID, GECOS field description, home directory, and login shell:

```
#Type Name     ID           GECOS                Home directory Shell
u    httpd    404          "HTTP User"
u    authd    /usr/bin/authd "Authorization user"
u    postgres −            "Postgresql Database" /var/lib/pgsql /libexec/postgresdb
g    input    −            −
m    authd    input
u    root     0            "Superuser"          /root         /bin/zsh
```

Empty lines and lines beginning with the "#" character are ignored, and may be used for commenting.

Type

The type consists of a single letter. The following line types are understood:

u

Create a system user and group of the specified name should they not exist yet. The user's primary group will be set to the group bearing the same name. The account will be created disabled, so that logins are not allowed.

g

Create a system group of the specified name should it not exist yet. Note that *u* implicitly create a matching group. The group will be created with no password set.

m

Add a user to a group. If the user or group do not exist yet, they will be implicitly created.

r

Add a range of numeric UIDs/GIDs to the pool to allocate new UIDs and GIDs from. If no line of this

type is specified, the range of UIDs/GIDs is set to some compiled−in default. Note that both UIDs and GIDs are allocated from the same pool, in order to ensure that users and groups of the same name are likely to carry the same numeric UID and GID.

Name

The name field specifies the user or group name. The specified name must consist only of the characters a−z, A−Z, 0−9, "_" and "−", except for the first character which must be one of a−z, A−Z or "_" (i.e. numbers and "−" are not permitted as first character). The user/group name must have at least one character, and at most 31.

It is strongly recommended to pick user and group names that are unlikely to clash with normal users created by the administrator. A good scheme to guarantee this is by prefixing all system and group names with the underscore, and avoiding too generic names.

For *m* lines, this field should contain the user name to add to a group.

For lines of type *r*, this field should be set to "−".

ID

For *u* and *g*, the numeric 32−bit UID or GID of the user/group. Do not use IDs 65535 or 4294967295, as they have special placeholder meanings. Specify "−" for automatic UID/GID allocation for the user or group (this is strongly recommended unless it is strictly necessary to use a specific UID or GID). Alternatively, specify an absolute path in the file system. In this case, the UID/GID is read from the path's owner/group. This is useful to create users whose UID/GID match the owners of pre−existing files (such as SUID or SGID binaries). The syntax "*uid*:*gid*" is also supported to allow creating user and group pairs with different numeric UID and GID values. The group with the indicated GID must get created explicitly before or it must already exist. Specifying "−" for the UID in this syntax is also supported.

For *m* lines, this field should contain the group name to add to a user to.

For lines of type *r*, this field should be set to a UID/GID range in the format "FROM−TO", where both values are formatted as decimal ASCII numbers. Alternatively, a single UID/GID may be specified formatted as decimal ASCII numbers.

GECOS

A short, descriptive string for users to be created, enclosed in quotation marks. Note that this field may not contain colons.

Only applies to lines of type *u* and should otherwise be left unset (or "−").

Home Directory

The home directory for a new system user. If omitted, defaults to the root directory.

Only applies to lines of type *u* and should otherwise be left unset (or "−"). It is recommended to omit this, unless software strictly requires a home directory to be set.

Shell

The login shell of the user. If not specified, this will be set to /usr/sbin/nologin, except if the UID of the user is 0, in which case /bin/sh will be used.

Only applies to lines of type *u* and should otherwise be left unset (or "−"). It is recommended to omit this, unless a shell different /usr/sbin/nologin must be used.

SPECIFIERS

Specifiers can be used in the "Name", "ID", "GECOS", "Home directory", and "Shell" fields. An unknown or unresolvable specifier is treated as invalid configuration. The following expansions are understood:

Table 1. Specifiers available

Specifier	Meaning	Details
"%b"	Boot ID	The boot ID of the running system, formatted as string. See **random**(4) for more information.
"%H"	Host name	The hostname of the running system.
"%m"	Machine ID	The machine ID of the running system, formatted as string. See **machine-id**(5) for more information.
"%T"	Directory for temporary files	This is either /tmp or the path "$TMPDIR", "$TEMP" or "$TMP" are set to.
"%v"	Kernel release	Identical to **uname −r** output.
"%V"	Directory for larger and persistent temporary files	This is either /var/tmp or the path "$TMPDIR", "$TEMP" or "$TMP" are set to.
"%%"	Escaped "%"	Single percent sign.

IDEMPOTENCE

Note that **systemd−sysusers** will do nothing if the specified users or groups already exist or the users are members of specified groups, so normally there is no reason to override sysusers.d vendor configuration, except to block certain users or groups from being created.

SEE ALSO

systemd(1), **systemd-sysusers**(8)