

**NAME**

nfsidmap – The NFS idmapper upcall program

**SYNOPSIS**

```
nfsidmap [-v] [-t timeout] key desc
nfsidmap [-v] [-c]
nfsidmap [-v] [-u|-g|-r user]
nfsidmap -d
nfsidmap -l
nfsidmap -h
```

**DESCRIPTION**

The NFSv4 protocol represents the local system's UID and GID values on the wire as strings of the form *user@domain*. The process of translating from UID to string and string to UID is referred to as "ID mapping."

The system derives the *user* part of the string by performing a password or group lookup. The lookup mechanism is configured in */etc/idmapd.conf*.

By default, the *domain* part of the string is the system's DNS domain name. It can also be specified in */etc/idmapd.conf* if the system is multi-homed, or if the system's DNS domain name does not match the name of the system's Kerberos realm.

The */usr/sbin/nfsidmap* program performs translations on behalf of the kernel. The kernel uses the request-key mechanism to perform an upcall. */usr/sbin/nfsidmap* is invoked by */sbin/request-key*, performs the translation, and initializes a key with the resulting information. The kernel then caches the translation results in the key.

*nfsidmap* can also clear cached ID map results in the kernel, or revoke one particular key. An incorrect cached key can result in file and directory ownership reverting to "nobody" on NFSv4 mount points.

In addition, the **-d** and **-l** options are available to help diagnose misconfigurations. They have no effect on the keyring containing ID mapping results.

**OPTIONS**

- c** Clear the keyring of all the keys.
- d** Display the system's effective NFSv4 domain name on *stdout*.
- g user** Revoke the gid key of the given user.
- h** Display usage message.
- l** Display on *stdout* all keys currently in the keyring used to cache ID mapping results. These keys are visible only to the superuser.
- r user** Revoke both the uid and gid key of the given user.
- t timeout**  
Set the expiration timer, in seconds, on the key. The default is 600 seconds (10 mins).
- u user** Revoke the uid key of the given user.
- v** Increases the verbosity of the output to syslog (can be specified multiple times).

**CONFIGURING**

The file */etc/request-key.conf* will need to be modified so */sbin/request-key* can properly direct the upcall. The following line should be added before a call to `keyctl negate`:

```
create id_resolver * * /usr/sbin/nfsidmap -t 600 %k %d
```

This will direct all `id_resolver` requests to the program */usr/sbin/nfsidmap*. The **-t 600** defines how many seconds into the future the key will expire. This is an optional parameter for */usr/sbin/nfsidmap* and will default to 600 seconds when not specified.

The idmapper system uses four key descriptions:

uid: Find the UID for the given user  
gid: Find the GID for the given group  
user: Find the user name for the given UID  
group: Find the group name for the given GID

You can choose to handle any of these individually, rather than using the generic upcall program. If you would like to use your own program for a uid lookup then you would edit your request-key.conf so it looks similar to this:

```
create id_resolver uid:* * /some/other/program %k %d
create id_resolver * * /usr/sbin/nfsidmap %k %d
```

Notice that the new line was added above the line for the generic program. request-key will find the first matching line and run the corresponding program. In this case, /some/other/program will handle all uid lookups, and /usr/sbin/nfsidmap will handle gid, user, and group lookups.

## FILES

*/etc/idmapd.conf*  
ID mapping configuration file

*/etc/request-key.conf*  
Request key configuration file

## SEE ALSO

[idmapd.conf\(5\)](#), [request-key\(8\)](#)

## AUTHOR

Bryan Schumaker, <bjschuma@netapp.com>