NAME

nisaddcred – create NIS+ credentials

SYNOPSIS

nisaddcred [**–p** *principal*] [**–P** *nis_principal*] [**–l** *login_password*] *auth_type* [*domain_name*]

nisaddcred **–r** [*nis_principal*] [*domain_name*]

AVAILABILITY

SUNWnisu

DESCRIPTION

The **nisaddcred** command is used to create security credentials for NIS+ principals. NIS+ credentials serve two purposes. The first is to provide authentication information to various services; the second is to map the authentication service name into a NIS+ principal name.

When the **nisaddcred** command is run, these credentials get created and stored in a table named **cred.org_dir** in the default NIS+ domain. If *domain_name* is specified, the entries are stored in the **cred.org_dir** of the specified domain. The specified domain must either be the one to which you belong, or one in which you are authenticated and authorized to create credentials, i.e., a subdomain. Note that the credentials of normal users must be stored in the same domain as their passwords.

It is simpler to add credentials using **nisclient**(1M), because it obtains the required information itself. **nispopulate**(1M) is used for "bulk" updates and can also be used to add credentials for entries in the **hosts** and the **passwd** NIS+ tables.

NIS+ principal names are used in specifying clients that have access rights to NIS+ objects. For more details, refer to the "Principal Names" subsection of the **nis+**(1) manual page. See **nischmod**(1), **nischown**(1), **nis_objects**(3N), and **nis_groups**(3N). Various other services can also implement access control based on these principal names.

The **cred.org_dir** table is organized as follows :

cname	auth_type	auth_name	public_data	private_data
user1.foo.com.	LOCAL	2990	10,102,44	
user1.foo.com.	DES	unix.2990@foo.com	098...819	3b8...ab2

The **cname** column contains a canonical representation of the NIS+ principal name. By convention, this name is the login name of a user, or the host name of a machine, followed by a dot ('.') followed by the fully qualified "home" domain of that principal. For users, the home domain is defined to be the domain where their DES credentials are kept. For hosts, their home domain is defined to be the domain name returned by the **domainname**(1M) command executed on that host.

There are two types of *auth_type* entries in the **cred.org_dir** table. Those with authentication type LOCAL, and those with authentication type DES. *auth_type*, specified on the command line in upper or lower case, should be either *local* or *des*.

Entries of type LOCAL are used by the NIS+ service to determine the correspondence between fully qualified NIS+ principal names and users identified by UIDs in the domain containing the **cred.org_dir** table.

This correspondence is required when associating requests made using the **AUTH_SYS** RPC authentication flavor (see **rpc_clnt_auth**(3N)) to a NIS+ principal name. It is also required for mapping a UID in one domain to its fully qualified NIS+ principal name whose home domain may be elsewhere. The principal's credentials for any authentication flavor may then be sought for within the **cred.org_dir** table in the principal's home domain (extracted from the principal name). The same NIS+ principal may have LOCAL credential entries in more than one domain. Only users, and not machines, have LOCAL credentials. In their home domain, users of NIS+ should have both types of credentials.

The *auth_name* associated with the LOCAL type entry is a UID that is valid for the principal in the domain containing the **cred.org_dir** table. This may differ from that in the principal's home domain. The public information stored in *public_data* for this type contains a list of GIDs for groups in which the user is a member. The GIDs also apply to the domain in which the table resides. There is no private data associated with this type. Neither a UID nor a principal name should appear more than once among the LOCAL entries in any one **cred.org_dir** table.

The DES *auth_type* is used for Secure RPC authentication (see **secure_rpc**(3N)).

The authentication name associated with the DES *auth_type* is a Secure RPC *netname*. A Secure RPC netname has the form **unix.***id@domain.com,* where *domain* must be the same as the domain of the principal. For principals that are users the *id* must be the UID of the principal in the principal's home domain. For principals that are hosts, the *id* is the host's name. In Secure RPC, processes running under effective UID 0 (root) are identified with the host principal. Unlike LOCAL, there cannot be more than one DES credential entry for one NIS+ principal in the NIS+ namespace.

The public information in an entry of authentication type DES is the public key for the principal. The private information in this entry is the private key of the principal encrypted by the principal's network password.

User clients of NIS+ should have credentials of both types in their home domain. In addition, a principal must have a LOCAL entry in the **cred.org_dir** table of each domain from which the principal wishes to make authenticated requests. A client of NIS+ that makes a request from a domain in which it does not have a LOCAL entry will be unable to acquire DES credentials. A NIS+ service running at security level 2 or higher will consider such users unauthenticated and assign them the name *nobody* for determining access rights.

This command can only be run by those NIS+ principals who are authorized to add or delete the entries in the **cred** table.

If credentials are being added for the caller itself, **nisaddcred** automatically performs a keylogin for the caller.

You can list the **cred** entries for a particular principal with **nismatch**(1).

OPTIONS

−p *principal*
The name *principal* specifies the name of the principal as defined by the naming rules for that specific mechanism. For example, LOCAL credential names are supplied with this option by including a string specifying a UID. For DES credentials, the name should be a Secure RPC netname of the form **unix.***id@domain.com,* as described earlier. If the **−p** option is not

specified, the *auth_name* field is constructed from the effective UID of the current process and the name of the local domain.

–P *nis_principal* Use the NIS+ principal name *nis_principal*. This option should be used when creating LOCAL or DES credentials for users whose home domain is different than the local machine's default domain.

Whenever the –**P** option is not specified, **nisaddcred** constructs a principal name for the entry as follows. When it is not creating an entry of type LOCAL, **nisaddcred** calls **nis_local_principal**, which looks for an existing LOCAL entry for the effective UID of the current process in the **cred.org_dir** table and uses the associated principal name for the new entry. When creating an entry of authentication type LOCAL, **nisaddcred** constructs a default NIS+ principal name by taking the login name of the effective UID for its own process, and appending to it a dot ('.') followed by the local machine's default domain. If the caller is a superuser, the machine name is used instead of the login name.

–l *login_password*
Use the *login_password* specified as the password to encrypt the secret key for the credential entry. This overrides the prompting for a password from the shell. This option is intended for administration scripts only. Prompting guarantees not only that no one can see your password on the command line using **ps**(1) but it also checks to make sure you have not made any mistakes. **NOTE:** *login_password* does not really HAVE to be the user's password but if it is, it simplifies logging in.

–r [*nis_principal*]
Remove all credentials associated with the principal *nis_principal* from the **cred.org_dir** table. This option can be used when removing a client or user from the system. If *nis_principal* is not specified the default is to remove credentials for the current *user*. If *domain_name* is not specified, the operation is executed in the default NIS+ domain.

EXIT CODES

This command returns **0** on success and **1** on failure.

EXAMPLES

The following examples illustrate how to add the LOCAL and DES credentials for some user, user1, with a UID of **2990**, who is an NIS+ user principal in the **some.domain.com.** NIS+ domain.

```
example% nisaddcred –p 2990 \
        –P user1.some.domain.com. local
```

Note that credentials are always added in the **cred.org_dir** table in the domain where **nisaddcred** is run, unless *domain_name* is specified as the last parameter on the command line. If credentials are being added from the domain server for its clients, then *domain_name* should be specified. The caller should have adequate permissions to create entries in the **cred.org_dir** table.

The system administrator can add a DES credential for the same user, using the following example:

**example% nisaddcred −p unix.2990@some.domain.com **
−P user1.some.domain.com. des

Please note that DES credentials can be added only after the LOCAL credentials have been added.

Note that the secure RPC netname does not end with a dot ('.') while the NIS+ principal name (specified with the −**P** option) does. This command should be executed from a machine in the same domain as is the user.

The following example shows how to add a machine's DES credentials in the same domain.

**example% nisaddcred −p unix.foo@some.domain.com **
−P foo.some.domain.com. des

Please note that no LOCAL credentials are needed in this case.

The following example illustrates how to add a NIS+ workstation's principal DES credential.

**example% nisaddcred −p unix.host1@sub.some.domain.com **
−P newhost.sub.some.domain.com. des sub.some.domain.com.

This format is particularly useful if you are running this command from a server which is in a higher domain than sub.some.domain.com. Without the last option for domain name, **nisaddcred** would fail because it would attempt to use the default domain of some.domain.com.

The following example illustrates adding DES credentials without being prompted for the root login password.

**example% nisaddcred −p unix.2990@some.domain.com **
−P user1.some.domain.com. -l *login_password* **des**

SEE ALSO

chkey(1), **keylogin**(1), **nis+**(1), **nischmod**(1), **nischown**(1), **nismatch**(1), **nistbladm**(1), **ps**(1), **domainname**(M), **nisclient**(1M), **nispopulate**(1M), **nis_local_names**(3N), **rpc_clnt_auth**(3N), **secure_rpc**(3N), **nis_objects**(3N), **nis_groups**(3N)

NOTES

The **cred.org_dir** NIS+ table replaces the maps *publickey.byname* and *netid.byname* used in NIS (YP).