PAM-Based Authentication

Linux

Linux clients can use the Pluggable Authentication Modules (PAM) to authenticate against LDAP Servers. The client must be configured to utilize PAM and connect with the LDAP Server. Below are the instructions necessary to accomplish both tasks.

Note: RedHat recommends SSSD, but can be configured to use PAM. The instructions to do so can be found here:

https://access.RedHat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/ch-Configuring_Authentication.html

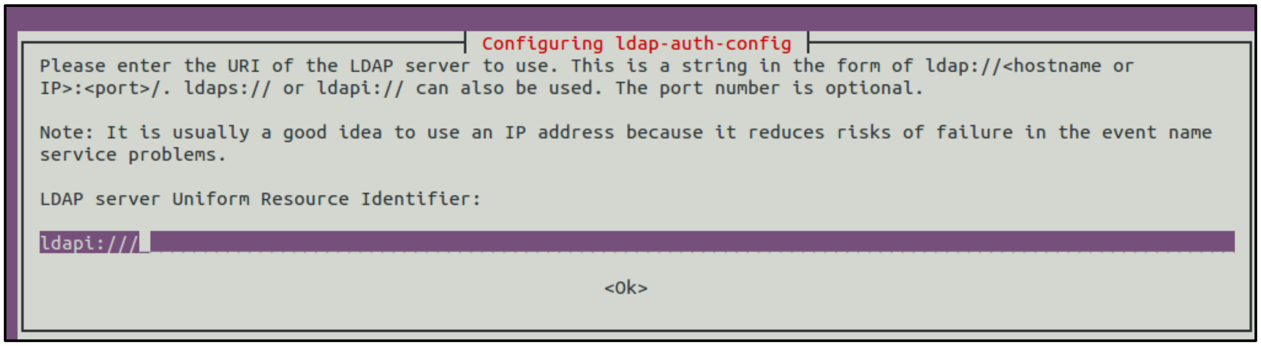
The following instructions apply only to Ubuntu/Debian.

1. To install the prerequisite software issue the following command:

```
sudo apt-get install ldap-utils libnss-ldapd ldap-auth-client nscd nslcd -y
```

(Installs to /etc/pam.d)

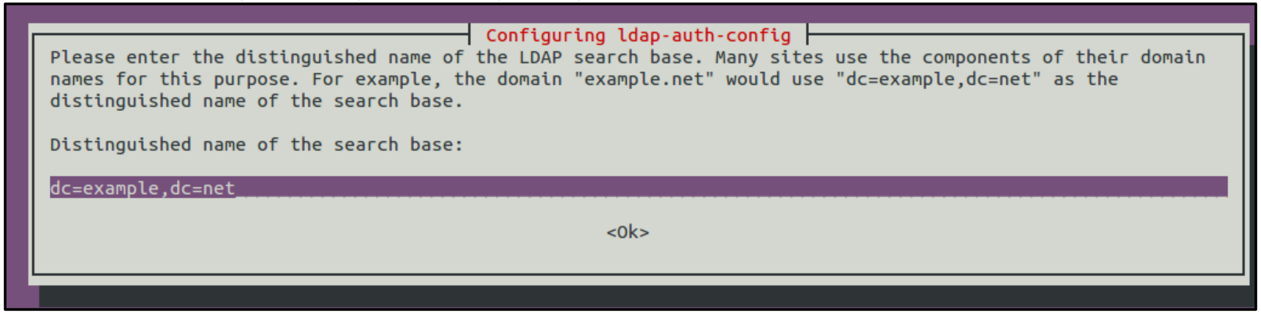
NOTE: During the installation of the above packages a dialog will pop up and ask about some LDAP configuration. Be sure to enter the correct values for your LDAP configuration.



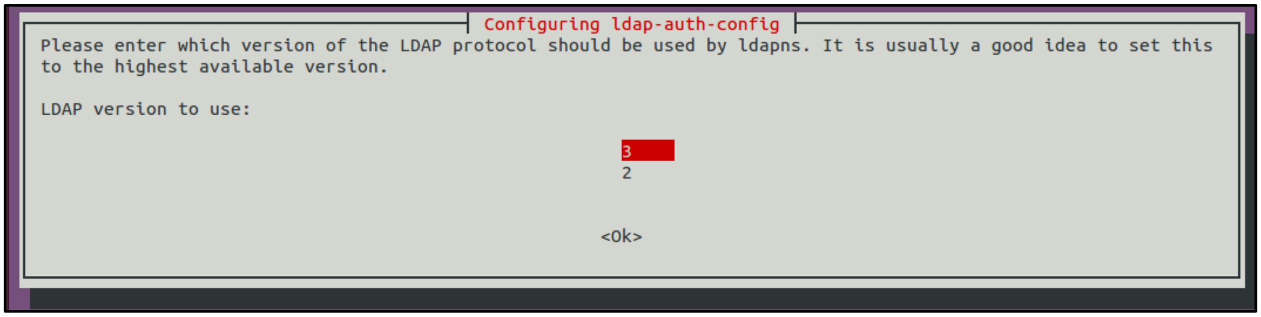
```
Configuring ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or
IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name
service problems.

LDAP server Uniform Resource Identifier:

ldapi:///

<Ok>
```

This needs to be the FQDN of the LDAP Server including port

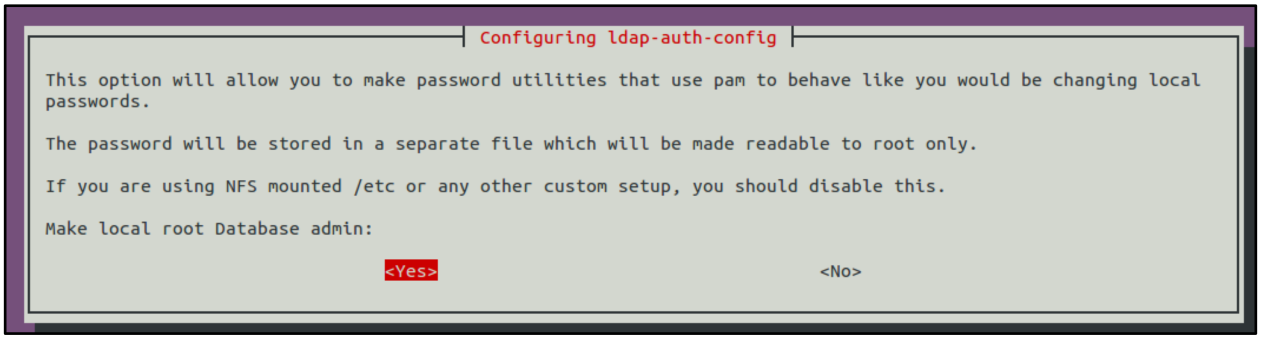
```
ldap://<ldapserver fqdn>:<port>/
```



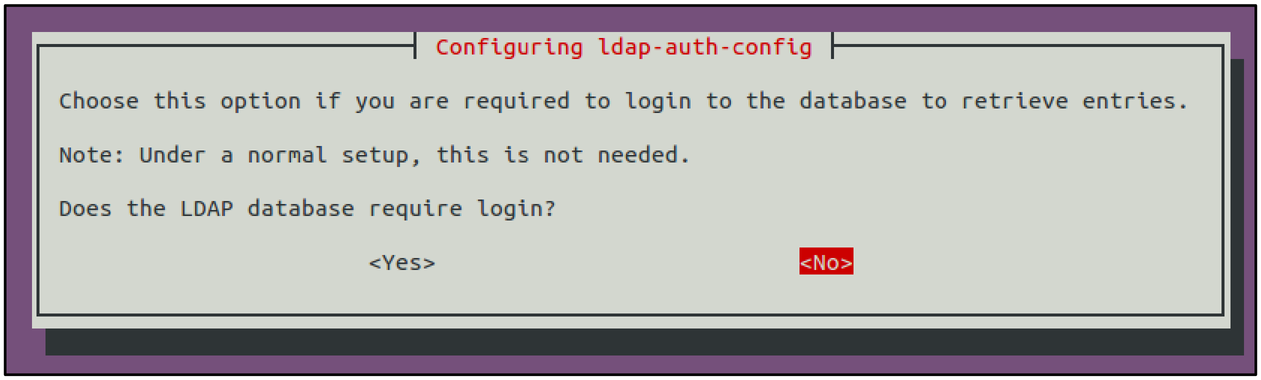
```
Configuring ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain
names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the
distinguished name of the search base.

Distinguished name of the search base:

dc=example,dc=net

<Ok>
```



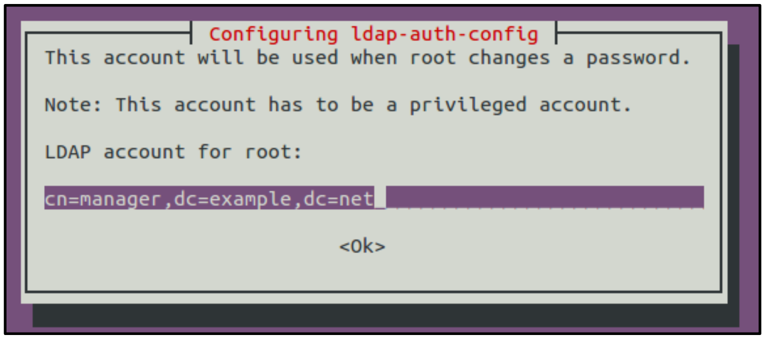
```
Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this
to the highest available version.

LDAP version to use:

                                        3
                                        2

                                      <Ok>
```



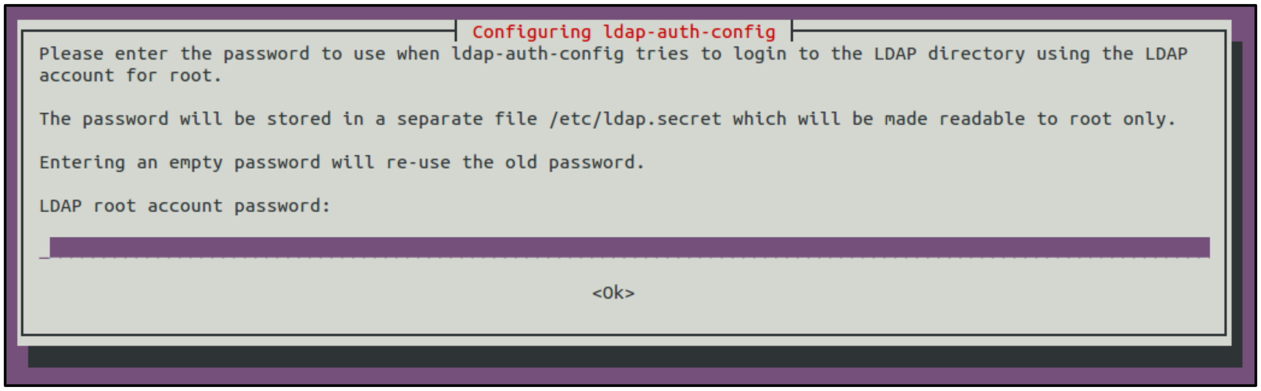
```
Configuring ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local
passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

                        <Yes>                                        <No>
```



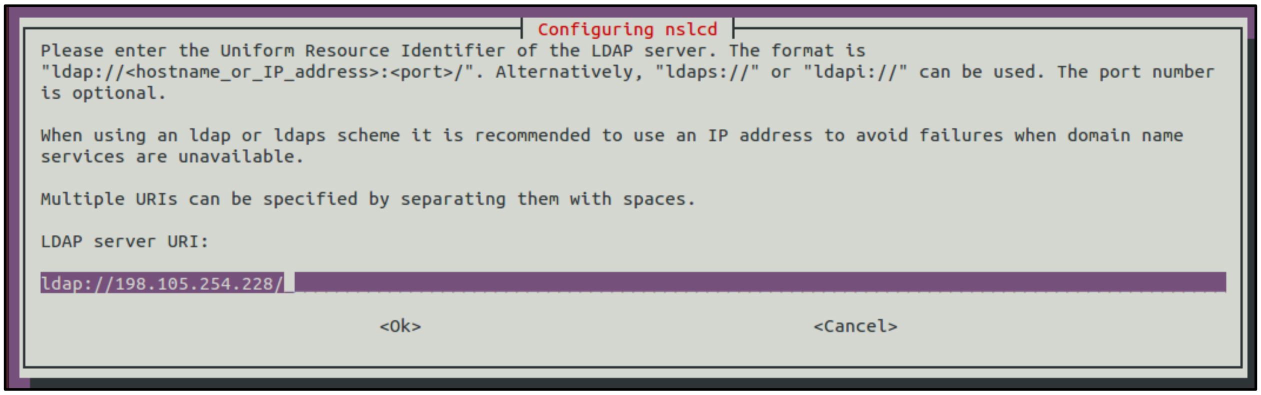
```
Configuring ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

                    <Yes>                         <No>
```



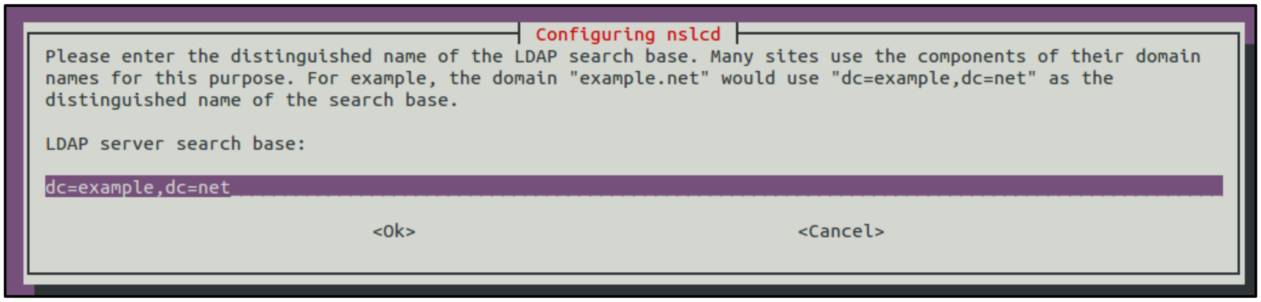
```
Configuring ldap-auth-config
This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

cn=manager,dc=example,dc=net_

                    <Ok>
```



```
Configuring ldap-auth-config
Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP
account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

_

                                        <Ok>
```



```
Configuring nslcd
Please enter the Uniform Resource Identifier of the LDAP server. The format is
"ldap://<hostname_or_IP_address>:<port>/". Alternatively, "ldaps://" or "ldapi://" can be used. The port number
is optional.

When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name
services are unavailable.

Multiple URIs can be specified by separating them with spaces.

LDAP server URI:

ldap://198.105.254.228/_

                       <Ok>                                   <Cancel>
```



```
Configuring nslcd
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain
names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the
distinguished name of the search base.

LDAP server search base:

dc=example,dc=net

                       <Ok>                                   <Cancel>
```

LDAP_AUTH_CLIENT

The meta-package called ldap-auth-client will install all required packages for an ldap client (auth-client-config, ldap-auth-config, libnss-ldap and libpam-ldap)

NSCD DESCRIPTION

nscd caches libc-issued requests to the Name Service. If retrieving NSS data is fairly expensive, nscd is able to speed up consecutive access to the same data dramatically and increase overall system performance. Nscd should be run at boot time by /etc/init.d/nscd.

NSLCD DESCRIPTION

nslcd is a daemon that will do LDAP queries for local processes that want to do user, group and other naming lookups (NSS) or do user authentication, authorization or password modification (PAM).

LIBNSS-LDAPD

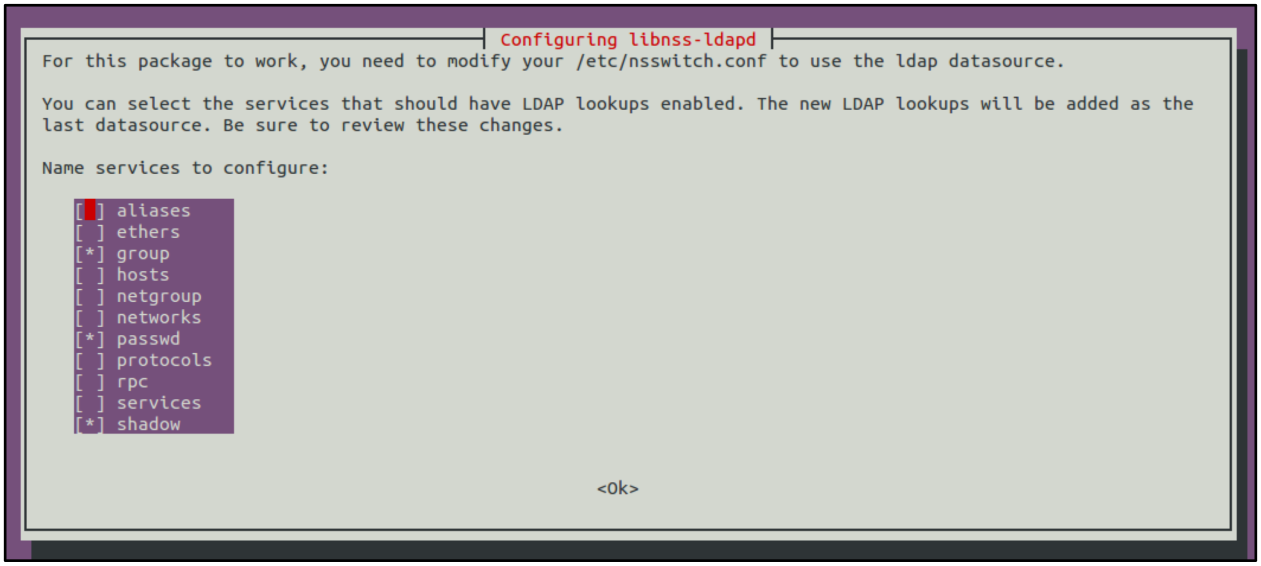
Configures NSSwitch to Use LDAP by commenting out the following lines:

```
passwd: compat
group : compat
shadow: compat
```

compat is a NIS_/etc/password hybrid that is highly compatible

And adding the following lines

```
passwd: files ldap
group: files ldap
shadow: files ldap
netgroup: nis
```



```
Configuring libnss-ldapd
For this package to work, you need to modify your /etc/nsswitch.conf to use the ldap datasource.

You can select the services that should have LDAP lookups enabled. The new LDAP lookups will be added as the
last datasource. Be sure to review these changes.

Name services to configure:

    [ ] aliases
    [ ] ethers
    [*] group
    [ ] hosts
    [ ] netgroup
    [ ] networks
    [*] passwd
    [ ] protocols
    [ ] rpc
    [ ] services
    [*] shadow

                                            <Ok>
```

2. Configure NS Services to Auto-Create Home directories as specified in LDAP Database
   Edit /etc/pam.d/login, /etc/pam.d/lightdm, /etc/pam.d/common-session (via sudo) and insert the following:

   ```
   session required pam_mkhomedir.so skel=/etc/skel umask=0022
   ```

   SKEL is a skeleton that is copied in recursively to where it is supposed to populate
   UMASK applies to the directory access permissions 755 for the user specified

3. Assign local groups to users
   To assign local groups to a domain (ldap) user do the following edit /etc/security/group.conf and add something like the following to it (log in as a local user and run the groups command to verify what to add):

   ```
   *;*;*;Al0000-2400;audio,cdrom,dialout,floppy
   ```

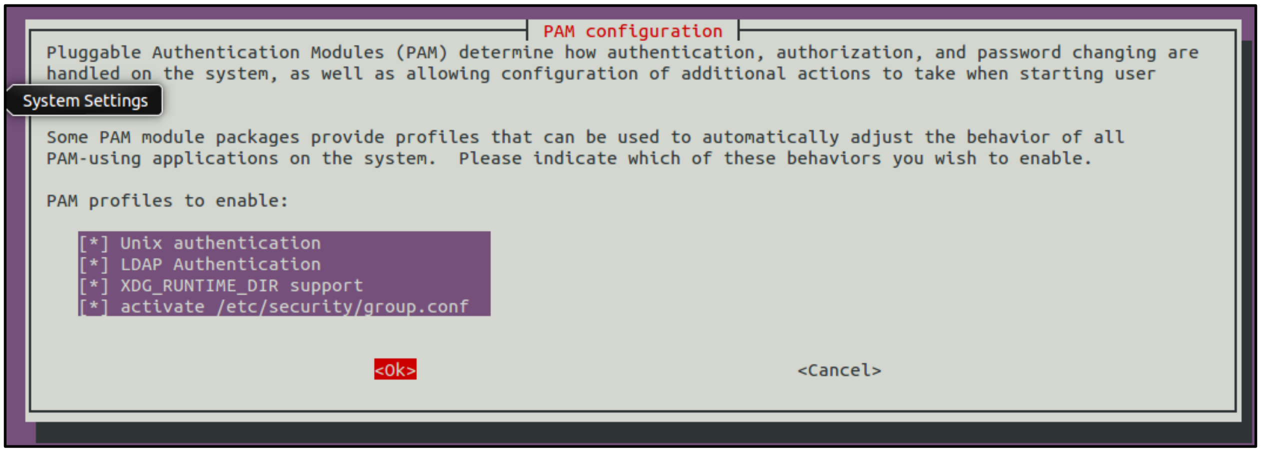
   In order to get the pam_group module working you could create a file like /usr/share/pam-configs/my_groups:

```
Name: activate /etc/security/group.conf
Default: yes
Priority: 900
Auth-Type: Primary
Auth:
        required                        pam_group.so use_first_pass
```

Activate the change by running the following:

```
pam-auth-update --force
```

Include "activate /etc/security/group.conf"



```
PAM configuration
Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are
handled on the system, as well as allowing configuration of additional actions to take when starting user

Some PAM module packages provide profiles that can be used to automatically adjust the behavior of all
PAM-using applications on the system.  Please indicate which of these behaviors you wish to enable.

PAM profiles to enable:

   [*] Unix authentication
   [*] LDAP Authentication
   [*] XDG_RUNTIME_DIR support
   [*] activate /etc/security/group.conf
```

This roughly equals editing /etc/pam.d/common-auth by hand and adding the following line before any pam_ldap and pam_krb5 settings:

```
auth     required      pam_group.so use_first_pass
```

You should now have local groups showing up for users logging in via gdm and ssh and can verify this by executing id or groups.

Finalize

Just to make sure everything works, run the following:

```
/etc/init.d/nscd restart
```

4. To ensure nslcd launches on bootup, issue this command:

```
sudo update-rc.d nslcd enable
```

5. You should be able to log in as an LDAP user after a reboot. If you don't reboot the machine, you must restart nslcd with:

```
/etc/init.d/nslcd restart
```

Common problems and solutions:

Logging in as an LDAP user takes a very long time (minutes): It's very likely that nss-lap is having problems finding the user's group. Make sure that the user is in a group recognized locally, or that the user is in a group defined in LDAP. Make sure that, if the group is defined in LDAP, that it's a real POSIX group.

- Always check the /var/log/auth.log log file. If you see "unable to contact ldap server", check whether the LDAP server is reachable and the port is open.
- Try to ping the LDAP server by name
- Try to check whether the LDAP port is open:

  LDAP can listen on different ports, but can usually be found on 389 and 636 which can be checked by using telnet:

  ```
  telnet <hostname (optional)> 389
  ```

  OR

  ```
  telnet <hostname (optional)> 636
  ```

  If you see any characters on the console then the port is open and the LDAP server should be running.

  If you see nothing or get an error message, either the LDAP server is not running or something (such as a firewall) is preventing the connection.

Solaris

System applications, like ssh, that use the PAM service are configured in the PAM configuration files.

See the pam.conf (https://docs.oracle.com/cd/E26502_01/html/E29042/pam.conf-4.html#REFMAN4pam.conf-4) man page for more information.

These configuration files include the /etc/pam.conf file, as well as service specific files placed in /etc/pam.d. Changes to these files affect all users on the system. The service specific PAM configuration files are the preferred mechanism for configuring PAM, since their granularity means a mistake in a file only affects that service. Also, adding new PAM services is simplified to copying a single file. The service specific files allow for better interoperability with other cross-platform PAM applications, since /etc/pam.d is the default configuration in most PAM implementations.

In addition, PAM policy files can be used to create authentication policies for individual services and assign those policies either to an individual, a group of individuals, or all users, as needed. The default PAM policy files are located in /etc/security/pam_policy. The PAM policy files provide the ability to set or change the authentication policy for one or more users in a safe and reliable manner.

The system administrator manages the PAM configuration files. An incorrect order of entries in these files can cause unforeseen side effects. For example, a badly configured file can lock out users so that single-user mode becomes necessary for repair. For a description of setting the order, see How PAM Stacking Works below.

PAM Configuration Search Order

The PAM configuration information in the PAM configuration files is collected by the PAM library in the following order:

1. The service name is looked for in /etc/pam.conf.
2. /etc/pam.d/*service* is checked.
3. The service name other is checked in /etc/pam.conf.
4. The /etc/pam.d/other file is checked.

This order allows for an existing /etc/pam.conf file to work with the per-service PAM configuration files located in /etc/pam.d.

PAM Configuration File Syntax

The /etc/pam.conf file and the PAM policy files use a syntax that is different than the service specific files. The entries in /etc/pam.conf or in PAM policy files are in one of the following formats:

```
service-name module-type control-flag module-path module-options
service-name module-type include path-to-included-PAM-configuration
```

service-name

The case insensitive name of the service, for example, login or passwd. An application can use different service names for the services that the application provides. For example, the Oracle Solaris secure shell daemon uses these service names: sshd-none, sshd-password, sshd-kbdint, sshd-pubkey, and sshd-hostbased. The service name other is a predefined name that is used as a wildcard service-name. If a particular service-name is not found in the configuration file, the configuration for other is used.

module-type

The type of service, that is, auth, account, session, or password.

control-flag

Indicates the role of the module in determining the integrated success or failure value for the service. Valid control flags are binding, definitive, include, optional, required, requisite, and sufficient. See How PAM Stacking Works below for information on the use of these flags.

module-path

The path to the library object that implements the service. If the pathname is not absolute, the pathname is assumed to be relative to /usr/lib/security/$ISA/. Use the architecture-dependent macro $ISA to cause libpam to look in the directory for the particular architecture of the application.

module-options

Options that are passed to the service modules. A module's man page describes the options that are accepted by that module. Typical module options include nowarn and debug.

path-to-included-PAM-configuration

Gives the full path to a separate PAM configuration file or a path name relative to the /usr/lib/security directory.

The per-service configuration files located in /etc/pam.d use the same syntax as pam.conf, but don't include the service name. When using the per-service configuration files, the name of the file is the service name. For instance, /etc/pam.d/cron includes the PAM configuration for the cron command.

How to Add a PAM Module

This procedure shows how to add a new PAM module. New modules can be created to cover site-specific security policies or to support third party applications.

Before You Begin: You must assume the root role. Determine which control flags and which options should be used. Refer to How PAM Stacking Works below for information on the control flags.

1. Ensure that the ownership and permissions are set so that the module file is owned by root and the permissions are 555.
2. Use pfedit to edit an appropriate PAM configuration file and add this module to the appropriate services.

Changes can be made to either /etc/pam.conf or /etc/pam.d/*service*.

3. Verify that the module has been added properly.

You must test in case the configuration file is misconfigured. Login using a direct service, such as ssh, and run the su command.

How to Log PAM Error Reports

Before You Begin: You must assume the root role.

1. Determine which system-log service instance is online.

```
svcs system-log
STATE          STIME       FMRI
disabled      13:11:55    svc:/system/system-log:rsyslog
online         13:13:27    svc:/system/system-log:default
```

2. Configure the /etc/syslog.conf file for the level of logging that you need.
   See the syslog.conf man page for more information about the logging levels (https://docs.oracle.com/cd/E26502_01/html/E29042/syslog.conf-4.html#REFMAN4syslog.conf-4). Most PAM error reporting is done to the LOG_AUTH facility.
3. Refresh the configuration information for the system-log service.

```
svcadm refresh system-log:default
```

Per User Authentication Policy

The pam_user_policy PAM module allows system administrators to specify PAM configurations on a per-user basis. The pam_policy key for the user needs to provide the path to a user-specific PAM configuration file. See the pam_user_policy (https://docs.oracle.com/cd/E26502_01/html/E29043/pam-user-policy-5.html#REFMAN5pam-user-policy-5) man page for more information.

Here are some ways to establish a per-user authentication policy:

- Create a new PAM policy file for a user and then use the usermod command to assign the policy to the user. Use the usermod command to assign a pre-defined policy to a user.
- Assign a rights profile that includes a pam_policy key to a user using the -P option to the usermod command.
- Assign a rights profile that includes a pam_policy key to all users by adding it to the PROFS_GRANTED key in /etc/security/policy.conf.

How to Assign a Customized PAM Policy to a User

Before You Begin: You must assume the root role.

1. Create a new PAM policy configuration file.

See the comments in the text below for a description of the effects of the file.

```
cat /etc/opt/pam_policy/custom-config
#
# PAM configuration which uses UNIX authentication for
console logins,
# LDAP for SSH keyboard-interactive logins, and denies
telnet logins.
#
login auth requisite          pam_authtok_get.so.1
login auth required           pam_dhkeys.so.1
login auth required           pam_unix_auth.so.1
login auth required           pam_unix_cred.so.1
login auth required           pam_dial_auth.so.1
#
sshd-kbdint  auth requisite          pam_authtok_get.so.1
sshd-kbdint   auth binding               pam_unix_auth.so.1
server_policy
sshd-kbdint  auth required           pam_unix_cred.so.1
sshd-kbdint  auth required           pam_ldap.so.1
#
telnet    auth     requisite    pam_deny.so.1
telnet    account  requisite    pam_deny.so.1
telnet    session  requisite    pam_deny.so.1
telnet    password requisite    pam_deny.so.1
```

2. Check the file permissions on the new file.
   The file must be owned by root and can not be group or world writable.

```
ls -l /etc/opt/pam_policy
total 5
-r--r--r--   1 root         4570 Jun 21 12:08 custom-config
```

3. Assign the new PAM policy to a user.
   The custom-config file in /etc/opt/pam_policy is assigned to the user named jill.

```
useradd -K pam_policy=/etc/opt/pam_policy/custom-config
jill
```

How to Assign a New Rights Profile to All Users

Before You Begin: You must assume the root role.

1. Create a new Rights Profile
   In this example, the ldap PAM policy is used.

```
profiles -p "PAM Per-User Policy of LDAP" \‘set
desc="Profile which sets pam_policy=ldap";
set pam_policy=ldap; exit;'
```

2. Assign the new Rights Profile to All Users
   Use pfedit to add the new policy to the PROFS_GRANTED declaration.

```
cat /etc/security/policy.conf
AUTHS_GRANTED=
PROFS_GRANTED=Basic Solaris User,PAM Per-User Policy of LDAP
CONSOLE_USER=Console User
```

Or assign the Rights Profile to a Single User

If a profile has been created as in step 1 in the previous procedure, that rights profile can be assigned to a user using the following command:

How Pam Stacking Works

When an application calls one of the following functions, libpam reads the PAM configuration files to determine which modules participate in the operation for this service:

- pam_authenticate(3PAM)
- pam_acct_mgmt(3PAM)
- pam_setcred(3PAM)
- pam_open_session(3PAM)
- pam_close_session(3PAM)
- pam_chauthtok(3PAM)

If the configuration files contain only one module for an operation for this service such as authentication or account management, the result of that module determines the outcome of the operation. For example, the default authentication operation for the passwd application contains one module, pam_passwd_auth.so.1:

```
passwd  auth required         pam_passwd_auth.so.1
```

If, on the other hand, there are multiple modules defined for the service's operation, those modules are said to be “stacked” and that a “PAM stack” exists for that service. For example, consider the case where /etc/pam.d/login contains the following entries:

```
auth definitive         pam_user_policy.so.1
auth requisite          pam_authtok_get.so.1
auth required           pam_unix_auth.so.1
auth required           pam_dhkeys.so.1
auth required           pam_unix_cred.so.1
auth required           pam_dial_auth.so.1
```

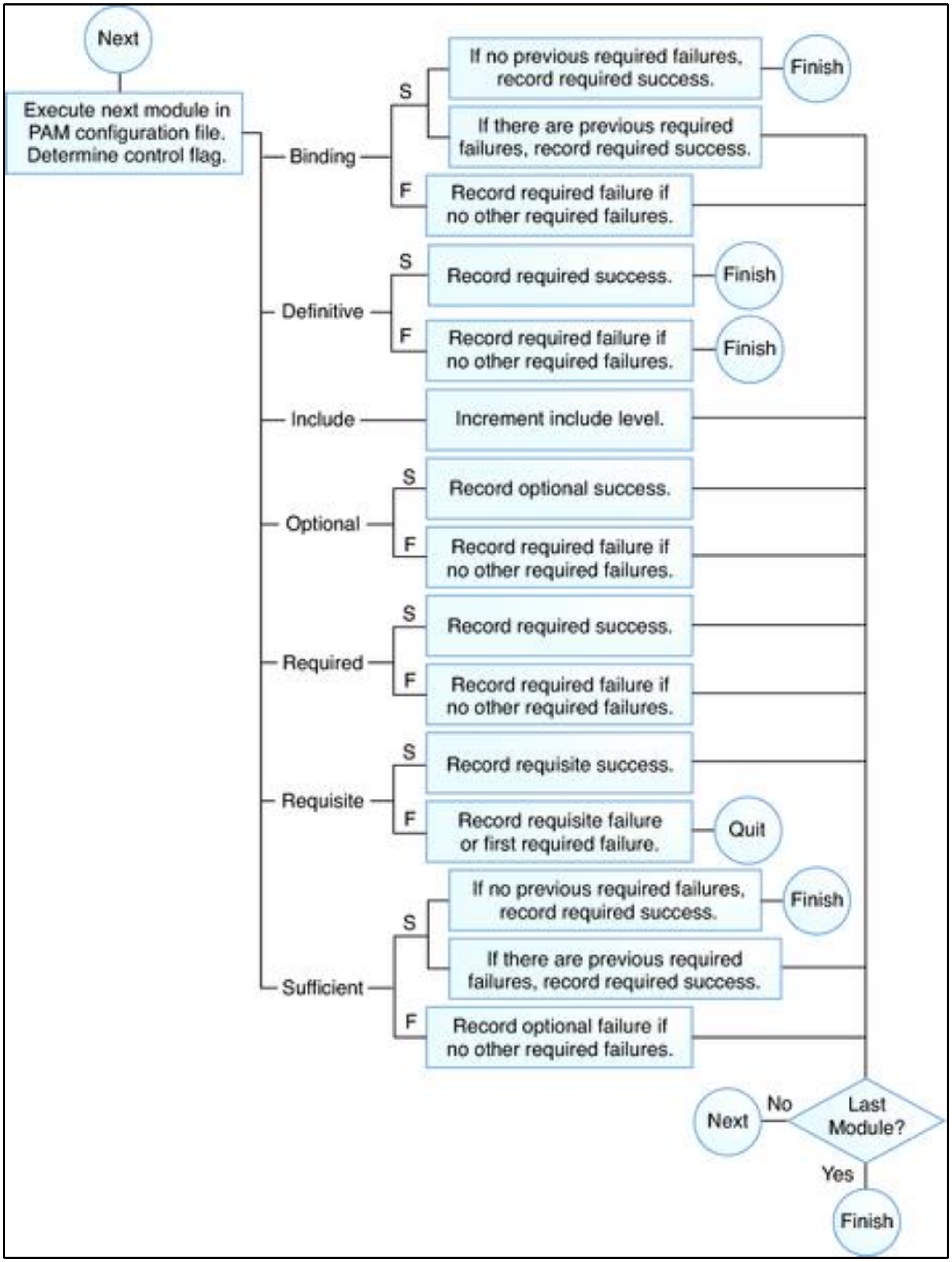
These entries represent a sample auth stack for the login service. To determine the outcome of this stack, the result codes of the individual modules require an integration process. In the integration process, the modules are executed in order as specified in the file. Each success or failure code is integrated in the overall result depending on the module's control flag. The control flag can cause early termination of the stack. For example, a requisite or definitive module might fail, or a sufficient, definitive, or binding module might succeed. After the stack has been processed, the individual results are combined into a single, overall result that is delivered to the application.

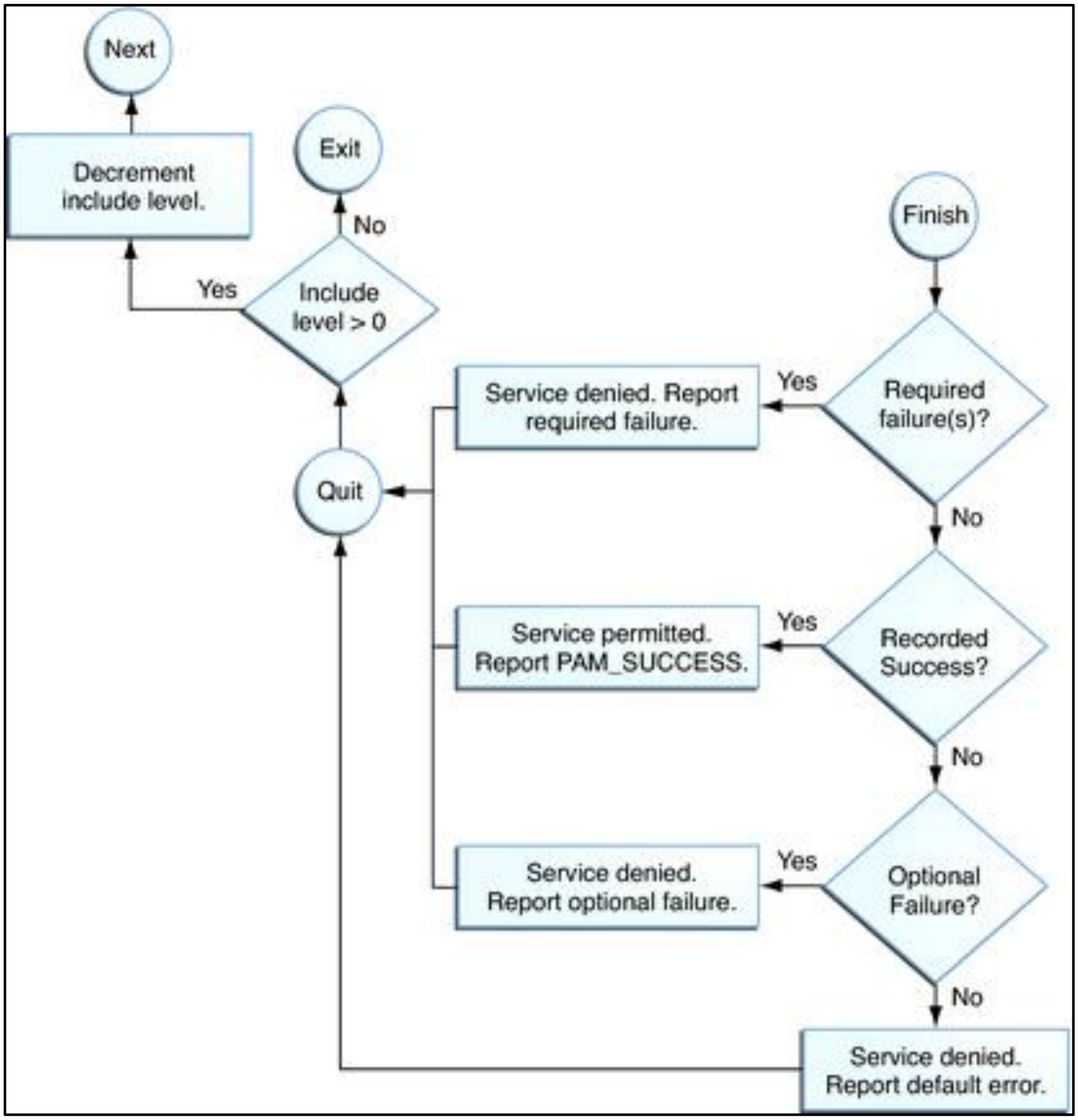
The control flag indicates the role that a PAM module plays in determining access to the service. The control flags and their effects are:

- ***Binding*** - Success in meeting a binding module's requirements returns success immediately to the application if no previous required modules have failed. If these conditions are met, then no further execution of modules occurs. Failure causes a required failure to be recorded and the processing of modules to be continued.
- ***Definitive*** - Success in meeting a definitive module's requirements returns success immediately to the application if no previous required modules have failed. If a previous required module failed, that failure is immediately returned to the application with no further execution of modules. Failure results in an immediate error return with no further execution of modules.

- ***Include*** - Adds lines from a separate PAM configuration file to be used at this point in the PAM stack. This flag does not control success or failure behaviors. When a new file is read, the PAM include stack is incremented. When the stack check in the new file finishes, the include stack value is decremented. When the end of a file is reached and the PAM include stack is 0, then the stack processing ends. The maximum number for the PAM include stack is 32.
- ***Optiona*l** - Success in meeting an optional module's requirements is not necessary for using the service. Failure causes an optional failure to be recorded.
- ***Required*** - Success in meeting a required module's requirements is necessary for using the service. Failure results in an error return after the remaining modules for this service have been executed. Final success for the service is returned only if no binding or required modules have reported failures.
- ***Requisite*** - Success in meeting a requisite module's requirements is necessary for using the service. Failure results in an immediate error return with no further execution of modules. All requisite modules for a service must return success for the function to be able to return success to the application.
- ***Sufficient*** - If no previous required failures have occurred, success in a sufficient module returns success to the application immediately with no further execution of modules. Failure causes an optional failure to be recorded.

The following two diagrams show how access is determined in the integration process. The first diagram indicates how success or failure is recorded for each type of control flag. The second diagram shows how the integrated value is determined.


Next
Execute next module in PAM configuration file. Determine control flag.
Binding
S
If no previous required failures, record required success.
Finish
If there are previous required failures, record required success.
F
Record required failure if no other required failures.
Definitive
S
Record required success.
Finish
F
Record required failure if no other required failures.
Finish
Include
Increment include level.
Optional
S
Record optional success.
F
Record required failure if no other required failures.
Required
S
Record required success.
F
Record required failure if no other required failures.
Requisite
S
Record requisite success.
F
Record requisite failure or first required failure.
Quit
Sufficient
S
If no previous required failures, record required success.
Finish
If there are previous required failures, record required success.
F
Record optional failure if no other required failures.
Next
No
Last Module?
Yes
Finish


Next
Decrement include level.
Exit
No
Yes
Include level > 0
Finish
Service denied. Report required failure.
Yes
Required failure(s)?
Quit
No
Service permitted. Report PAM_SUCCESS.
Yes
Recorded Success?
No
Service denied. Report optional failure.
Yes
Optional Failure?
No
Service denied. Report default error.

PAM Stacking Example

This example shows the default definitions for authentication management in the /etc/pam.d/other file. These definitions are used if no service-specific definitions have been configured.

```
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for
authentication
#
auth definitive         pam_user_policy.so.1
auth requisite          pam_authtok_get.so.1
auth required           pam_dhkeys.so.1
auth required           pam_unix_auth.so.1
auth required           pam_unix_cred.so.1
```

First, the security policy for the user is checked using the pam_user_policy module. The definitive control flag selects that if the evaluation of the security policy succeeds, the service returns success to the application, since no other modules have been checked at this point. If the request fails, then a failure message is sent to the application and no further checking is done. If no policy is set for the user, then the next module is executed.

If a per-user PAM policy isn't specified for this user, then the pam_authtok_get module is executed. The control flag for this module is set to requisite. If pam_authtok_get fails, then the authentication process ends and the failure is returned to the service.

If pam_authtok_get does not fail, then the next three modules are executed. These modules are configured with the required control flag, so that the process continues regardless of whether an individual failure is returned. After pam_unix_cred is executed, no modules remain. At this point, if all the modules succeeded, the user is granted access. If either pam_dhkeys, pam_unix_auth, or pam_unix_cred has returned a failure, the user is denied access.