NAME

pklocalauthority − PolicyKit Local Authority

DESCRIPTION

The Local Authority is the default PolicyKit authority implementation. Configuration for the Local Authority and information pertaining to authorization decisions are read from local files on the disk. One design goal of the Local Authority is to split configuration items into separate files such that 3rd party packages and users won't conflict trying to edit the same files. This policy also ensures smooth upgrades when distributing PolicyKit using a package management system.

Files shipped with PolicyKit and 3rd party packages (e.g. under package manager control) typically have comments (such as “DO NOT EDIT THIS FILE, it will be overwritten on update”) telling the system administrator that changes will be overwritten on update.

ADMINISTRATOR AUTHENTICATION

PolicyKit makes a distinction between *user authentication* (to make the user in front of the system prove he really is the user) and *administrator authentication* (to make the user in front of the system prove he really is an administrator). Since various operating systems (or even flavors of the same operating system) has different ways of defining "administrator", the Local Authority provides a way to specify what "administrator authentication" means.

By default, "administrator authentication" is defined as asking for the root password. Since some systems, for usability reasons, don't have a root password and instead rely on a group of users being member of an administrative group that gives them super−user privileges, the Local Authority can be configured to support this use−case as well.

Configuration for the Local Authority is read from files in the /etc/polkit−1/localauthority.conf.d directory. All files are read in lexigraphical order (using the C locale) meaning that later files can override earlier ones. The file 50−localauthority.conf contains the settings provided by the OS vendor. Users and 3rd party packages can drop configuration files with a priority higher than 60 to change the defaults. The configuration file format is simple. Each configuration file is a *key file* (also commonly known as a *ini file*) with a single group called [Configuration]. Only a single key, AdminIdentities is read. The value of this key is a semi−colon separated list of identities that can be used when administrator authentication is required. Users are specified by prefixing the user name with unix−user:, groups of users are specified by prefixing with unix−group:, and netgroups of users are specified with unix−netgroup:. See the section called “EXAMPLES” for an example of a configuration file.

DIRECTORY STRUCTURE

The Local Authority reads files with .pkla extension from all directories located inside the /etc/polkit−1/localauthority and /var/lib/polkit−1/localauthority directories. By default, the following sub−directories are installed.

```
/etc/polkit−1/
‘−− localauthority
   |−− 10−vendor.d
   |−− 20−org.d
   |−− 30−site.d
   |−− 50−local.d
   ‘−− 90−mandatory.d
```

and

```
/var/lib/polkit−1/
‘−− localauthority
   |−− 10−vendor.d
   |−− 20−org.d
   |−− 30−site.d
   |−− 50−local.d
```

```
‘−− 90−mandatory.d
```

The /etc/polkit−1/localauthority hierarchy is inteded for local configuration and the /var/lib/polkit−1/localauthority is intended for 3rd party packages.

Each .pkla file contains one or more authorization entries. If the underlying filesystem supports file monitoring, the Local Authority will reload information whenever .pkla files are added, removed or changed.

Each directory is intended for a specific audience

10−vendor.d
: Intended for use by the OS vendor.

20−org.d
: Intended for the organization deploying the OS.

30−site.d
: Intended for the site deploying the system.

50−local.d
: Intended for local usage.

90−mandatory.d
: Intended for the organization deploying the OS.

and new directories can be added/removed as needed.

As to regards to the content, each .pkla file is a standard *key file* and contains key/value pairs in one or more groups with each group representing an authorization entry. A .pkla file MUST be named by using a scheme to ensure that the name is unique, e.g. reverse DNS notation or similar. For example, if the organization is “Acme Corp” needs to modify policy for the product “Frobnicator”, a name like com.acme.frobnicator.pkla would be suitable.

AUTHORIZATION ENTRY

Each group in a .pkla file must have a name that is unique within the file it belongs to. The following keys are are recognized:

Identity
: A semi−colon separated list of globs to match identities. Each glob should start with unix−user: or unix−group: to specify whether to match on a UNIX user name or a UNIX group name. Netgroups are supported with the unix−netgroup: prefix, but cannot support glob syntax.

Action
: A semi−colon separated list of globs to match action identifiers.

ResultActive
: The result to return for subjects in an active local session that matches one or more of the given identities. Allowed values are similar to what can be used in the *defaults* section of .policy files used to define actions, e.g. yes, no, auth_self, auth_self_keep, auth_admin and auth_admin_keep.

ResultInactive
: Like *ResultActive* but instead applies to subjects in inactive local sessions.

ResultAny
: Like *ResultActive* but instead applies to any subject.

ReturnValue
: A semi−colon separated list of key/value pairs (of the form key=value) that are added to the details of authorization result on positive matches.

All keys specified above are required except that only at least one of *ResultAny*, *ResultInactive* and *ResultActive* must be present. The *ReturnValue* key is optional.

EVALUATION ORDER

When a Mechanism requests services from the Authority to check if a given Subject is authorized for a given Action, the authorization entries discussed above are consulted using the following algorithm.

The authorization entries from all .pkla files are ordered using the following rules. First all the basename of all sub−directories (e.g. *30−site.d*) from both the /etc/polkit−1/localauthority and /var/lib/polkit−1/localauthority directories are enumerated and sorted (using the C locale). If a name exists in both /etc and /var, the one in /etc takes precedence. Then all .pkla files are read in order from this list of sub−directories. For each .pkla file, authorizations from each file are appended in order resulting in an ordered list of authorization entries.

For example, given the following files

```
/var/lib/polkit−1
 localauthority
    10−vendor.d
   |  10−desktop−policy.pkla
    20−org.d
    30−site.d
    50−local.d
    55−org.my.company.d
   |  10−org.my.company.product.pkla
    90−mandatory.d

/etc/polkit−1
 localauthority
    10−vendor.d
   |  01−some−changes−from−a−subvendor.pkla
    20−org.d
    30−site.d
    50−local.d
    55−org.my.company.d
   |  10−org.my.company.product.pkla
    90−mandatory.d
```

the evaluation order of the .pkla files is:

1. 10−desktop−policy.pkla
2. 01−some−changes−from−a−subvendor.pkla
3. 10−org.my.company.product.pkla (the /var one)
4. 10−org.my.company.product.pkla (the /etc one)

When the list of authorization entries has been calculated, the authorization check can be made. First, the user of the Subject is determined and the groups that the user belongs are looked up. For each group identity, the authorization entries are consulted in order. If the authorization check matches the data from the authorization check, then the authorization result from *RequireAny*, *RequireInactive* or *RequireActive* is used and *ReturnValue* is added to the authorization result.

Finally, the authorization entries are consulted using the user identity in the same manner.

Note that processing continues even after a match. This allows for socalled “negative authorizations”, see the section called “EXAMPLES” for further discussion.

EXAMPLES

The following .conf file

```
[Configuration]
```

AdminIdentities=unix−group:staff

specifies that any user in the staff UNIX group can be used for authentication when administrator authentication is needed. This file would typically be installed in the /etc/polkit−1/localauthority.conf.d directory and given the name 60−desktop−policy.conf to ensure that it is evaluted after the 50−localauthority.conf file shipped with PolicyKit. If the local administrator wants to override this (suppose 60−desktop−policy.conf was shipped as part of the OS) he can simply create a file 99−my−admin−configuration.conf with the following content

[Configuration]
AdminIdentities=unix−user:lisa;unix−user:marge

to specify that only the users lisa and marge can authenticate when administrator authentication is needed.

The following .pkla file grants authorization to all users in the staff group for actions matching the glob com.example.awesomeproduct.* provided they are in an active session on the local console:

[Normal Staff Permissions]
Identity=unix−group:staff
Action=com.example.awesomeproduct.*
ResultAny=no
ResultInactive=no
ResultActive=yes

If the users homer and grimes are member of the staff group but policy requires that an administrator needs to authenticate every time authorization for any action matching com.example.awesomeproduct.* is required, one would add

[Exclude Some Problematic Users]
Identity=unix−user:homer;unix−user:grimes
Action=com.example.awesomeproduct.*
ResultAny=no
ResultInactive=no
ResultActive=auth_admin

and make sure this authorization entry is after the first one.

AUTHOR

Written by David Zeuthen <davidz@redhat.com> with a lot of help from many others.

BUGS

Please send bug reports to either the distribution or the polkit−devel mailing list, see the link **http://lists.freedesktop.org/mailman/listinfo/polkit-devel** on how to subscribe.

SEE ALSO

polkit(8)