Rocky Enterprise Linux 9.2 Manual Pages on command 'pkla-check-authorization.8'

$ man pkla-check-authorization.8

PKLA-CHECK-AUTHORI(8) pkla-check-authorization PKLA-CHECK-AUTHORI(8)

NAME

pkla-check-authorization - Evaluate pklocalauthority authorization configuration

SYNOPSIS

pkla-check-authorization [--help]

pkla-check-authorization [--paths paths] {user-name} {is-local} {is-active} {action}

DESCRIPTION

pkla-check-authorization interprets non-JavaScript configuration files described below to determine the response of polkit(8) to authorization queries.

Note: Authorization decision evaluation is driven by JavaScript rules as described in polkit(8). pkla-check-authorization is called by a JavaScript rule file named 49-polkit-pkla-compat.rules; other JavaScript rules with a higher priority may exist, so the pkla-check-authorization configuration may not necessarily govern the final polkit(8) authorization decision.

The ordering of the JavaScript rule files and the ordering of pkla-check-authorization configuration files is not integrated and uses different rules; the pkla-check-authorization configuration evaluation is happens at a single point within the JavaScript rule evaluation order.

pkla-check-authorization is an internal helper program of pkla-polkit-compat. You shouldn't need to run it directly, except for debugging purposes.

The arguments to pkla-check-authorization are, in order:

user-name

Name of the user account asking for authorization

is-local

Whether the attempted action is performed from a local login session, true or false.

is-active

Whether the attempted action is performed from a currently active session (e.g. currently active virtual console), true or false.

action

A string identifying the polkit(8) action.

If the configuration specifies an authorization decision, pkla-check-authorization outputs the decision and a terminating newline. If no decision is configured, the output is empty.

OPTIONS

-h, --help

Write a summary of the available options to standard output and exit successfully.

-p, --paths=paths

Search for configuration files in semicolon-separated paths instead of the default /var/lib/polkit-1/localauthority;/etc/polkit-1/localauthority.

EXIT STATUS

pkla-check-authorization exits with 0 on success (even if there is no decision configured), and a non-zero status on error.

DIRECTORY STRUCTURE

Files with .pkla extension are read from all directories located inside the /etc/polkit-1/localauthority and /var/lib/polkit-1/localauthority directories (or as specified using the --paths option). 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 intended 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 recognized:

Identity

A semi-colon separated list of entries to match identities. Each entry should start with unix-user: or unix-group: to specify whether to match on a UNIX user name or a UNIX group name, and continue with a glob matching the group or user name. Netgroups are supported with the unix-netgroup: prefix, but cannot support glob syntax. Finally, an entry "default" (with no prefix) can be used to specify the default match.

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.

All keys specified above are required except that only at least one of ResultAny, ResultInactive and ResultActive must be present.

EVALUATION ORDER

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. Then, authorization entries that include the "default" field value in the Identity field are consulted in order. If the authorization entry matches the data from the authorization check, then the authorization result from RequireAny, RequireInactive or RequireActive is used. Next, for each group identity, all authorization entries that contain a matching group entry are again consulted in the same manner. 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 so called ?negative authorizations?, see the section called ?EXAMPLE? for further discussion.

EXAMPLE

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.

The following entry modifies the default authorization decision (it is overridden by any entry that matches using unix-user: or unix-group:, but overrides any defaults set by the application author in an .action file):

[Disable Access by Default]

Identity=default

Action=com.example.awesomeproduct.*

ResultAny=no

ResultInactive=no

ResultActive=no

FILES

/etc/polkit-1/localauthority, /var/lib/polkit-1/localauthority

Default directories containing decision configuration files.

AUTHOR

Written by David Zeuthen <davidz@redhat.com> with a lot of help from many others. Adapted by Miloslav Trma? <mitr@redhat.com>.

SEE ALSO

polkit(8)

polkit-pkla-compat May 2013 PKLA-CHECK-AUTHORI(8)