

ACLs

Access Control Policies

A Rundeck *access control policy* grants users and user groups certain privileges to perform actions against rundeck resources like projects, jobs, nodes, commands and API. Every action requested by a user is evaluated by the Rundeck authorization system and logged for reporting and auditing purposes.

Since Rundeck respects the policy definition, you can define role-based authorization to restrict users to only a subset of actions. This enables a self-service type interface, where some users have access to a limited set of executable actions.

Two dimensions of information dictate authorization inside Rundeck:

- *group* memberships assigned to a *user* login.
- access control policy that grants access to one or more *policy actions* to a *group* or *user*.

Where can I edit the Policy?

This is done in the ACL Policy GUI or in the configuration file.

<https://docs.rundeck.com/docs/administration/security/acl-policy-editor.html>

Where and What are Access Control Policies?

Access to running or modifying Jobs is managed in an access control policy defined using the `aclpolicy` YAML document. This file contains a number of policy elements that describe what user group is allowed to perform which actions.

Please read over this document for information on how to define it, and how to grant access for certain actions to certain resources:

- `aclpolicy`

Policies can be organized into more than one file to help organize access by group or pattern of use. The normal Rundeck install will have generated a policy for the "admin" group. Not all users will need to be given "admin" access level to control and modify all Jobs. More typically, a group of users will be given access to just a subset of Jobs.

Lifecycle

The Rundeck server does not need to be restarted for changes to aclpolicy files to take effect.

Scopes

Revision #4

Created 14 December 2021 12:57:31 by jmoore53

Updated 12 January 2022 03:55:29 by andrewcz