General Permissions API Documentation

This documents the endpoints for the Permissions API which enables you to set permissions on objects in Databricks. Currently, you can set permissions on the following objects using these APIs - clusters, jobs, pools, notebooks and directories.

Note: This document includes examples for Service Principals. Service Principals support is currently in private preview in Azure Databricks.

Endpoint

```
$basepath/permissions/{$objectType + “s”}/$objectId

$basepath = /api/2.0/preview
```

```
{$objectType + “s”} is one of {clusters, instance-pools, jobs, notebooks,
directories, registered-models}
$objectId is the id for the corresponding objectType to modify
```

Get Possible Permission Levels

Retrieve Permissions on an Object

HTTP Verb: GET
Path: $basepath/permissions/{plural $objectType}/$objectId
Example Paths:

- $basepath/permissions/clusters/1235-245555-crows948
- $basepath/permissions/instance-pools/1258-564824-bugy123-pool-HLjdkEpH
- $basepath/permissions/jobs/1234
- $basepath/permissions/notebooks/108
- $basepath/permissions/directories/112
- $basepath/permissions/registered-models/1234-5678-9012-3456

General Response Body:

```
{
   "object_id": "/{$objectType + “s”}/$objectId",
   "object_type": "$objectType",
   "access_control_list": [
      {
         "user_name": "<User Name>" || "group_name": "<Group Name>" ||
"service_principal_name": "<Service Principal Name>",
         "all_permissions": [
            {
               "permission_level": "<PermissionLevel>",
               "inherited": true || false,
               "inherited_from_object": ["<$ObjectSourceId>"]
            }
         ]
      }
   ]
}
```

For Clusters:
Example Response:

```
{
   "object_id": "/clusters/1234-123456-mycluster0",
   "object_type": "cluster",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_RESTART",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/clusters/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

For Instance Pools:

Example Response:

```
{
   "object_id": "/instance-pools/0627-190120-two15-pool-6wmqH7IJ",
   "object_type": "instance-pool",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_ATTACH_TO",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/instance-pools/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

For Jobs:

```
{
   "object_id": "/jobs/123",
   "object_type": "job",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_VIEW",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/jobs/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

For Notebooks:

```
{
   "object_id": "/notebooks/108",
   "object_type": "notebook",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_VIEW",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/directories/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

For Directories:

```
{
   "object_id": "/directories/112",
   "object_type": "directory",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_RUN",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/directories/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

For Registered Models:

```
{
   "object_id": "/registered-models/1234-5678-9012-3456",
   "object_type": "registered-model",
   "access_control_list": [
      {
         "user_name": "user@mydomain.com",
         "all_permissions": [
            {
               "permission_level": "CAN_EDIT",
               "inherited": false
            },
            {...}
         ]
      },
      {
         "group_name": "admins",
         "all_permissions": [
            {
               "permission_level": "CAN_MANAGE",
               "inherited": true,
               "inherited_from_object": [
                  "/registered-models/"
               ]
            }
         ]
      },
      {...}
   ]
}
```

Add or Modify Permissions on an Object

HTTP Verb: PATCH

Path: $basepath/permissions/{plural $objectType}/$objectId

Example Paths:

- $basepath/permissions/clusters/1235-245555-crows948
- $basepath/permissions/instance-pools/1258-564824-bugy123-pool-HLjdkEpH
- $basepath/permissions/jobs/1234
- $basepath/permissions/notebooks/108
- $basepath/permissions/directories/112
- $basepath/permissions/registered-models/1234-5678-9012-3456

General Request Body:

```
{
   "access_control_list": [
      {
         "user_name":"<UserName>" || "group_name":"<GroupName>" ||
"service_principal_name": "<Service Principal Name>",
         "permission_level": "<PermissionLevel>"
      }
   ]
}
```

Response Body: Same as a GET call except with the updated permissions in the request.

Set or Delete Permissions on an Object

A PUT request will replace all direct permissions on the cluster object. Delete requests can be made by making a GET request to retrieve the current list of permissions followed by a PUT request by removing entries to be deleted.

HTTP Verb: PUT

Path: $basepath/permissions/{plural $objectType}/$objectId

Example Paths:

- $basepath/permissions/clusters/1234-mycluster
- $basepath/permissions/clusters/my-second-cluster
- $basepath/permissions/instance-pools/pool-id
- $basepath/permissions/registered-models/1234-5678-9012-3456

Request Body:

```
{
   "access_control_list": [
      {
         "user_name":"<UserName>" || "group_name":"<GroupName>" ||
"service_principal_name": "<Service Principal Name>",
         "permission_level": "<PermissionLevel>
      }
   ]
}
```

Response Body: Same as a GET call except with the updated permissions in the request.

PermissionLevel Enum

Name	Allowed Objects
CAN_MANAGE	Clusters, Instance-pools, Jobs, Notebooks, Directories, Registered Models
CAN_RESTART	Clusters
CAN_ATTACH_TO	Clusters, Instance-pools
CAN_MANAGE_RUN	Jobs
IS_OWNER	Jobs
CAN_VIEW	Jobs

CAN_READ	Notebooks, Directories, Registered Models
CAN_RUN	Notebooks, Directories
CAN_EDIT	Notebooks, Directories, Registered Models

These permission levels correlate directly to the permissions that you can configure in the UI. For details on the abilities associated with these permission levels, check the following links:

- Clusters
- Jobs
- Instance pools
- Notebooks
- Directories

You can use the following endpoint to fetch permission levels for different objects:

```
$basepath/permissions/{plural $objectType}/$objectId/permissionLevels

where $basepath = /api/2.0/preview
```

PermissionsDescription Object

Attribute Name	Type	Description
permissionLevel	PermissionLevel	Any given permission level
description	String	Description of the given permission level on the object type that is being queried

PermissionsRequest Object

Attribute Name	Type	Description
access_controL_list	List[AccessControlRequest]	List of all permission that are to be set on this ACL object for a specific principal

PermissionsResponse Object

Attribute Name	Type	Description

object_id	String	Id of the object where the permissions were set on. See How to get Workspace, Cluster, Notebook, and Job Details for where to find object ids.
object_type	String	Type of the object where the permissions were set on.
access_controL_list	List[AccessControlRequest]	List of all the lists of permissions set on this specific ACL object for various principals.

AccessControlRequest Object

Attribute Name	**Type**	**Description**
user_name || group_name || service_principal_name	String	Name of the principal (user or group) that has permissions set on the ACL object **user_name example:** user@databricks.coms
all_permissions	PermissionLevel	The permission level that is to be set on this ACL object for a specific principal

AccessControlResponse Object

Attribute Name	**Type**	**Description**
user_name || group_name || service_principal_name	String	Name of the principal (user or group) that has permissions set on the ACL object **user_name example:** user@databricks.coms
all_permissions	List[Permission]	List of all permission that are set on this ACL object for a specific principal This list includes both

		permissions directly set on this ACL object and permissions which are inherited from an ancestor ACL object

Permission Object

Attribute Name	**Type**	**Description**
permission_level	String	The name of the permission levels (see section below)
inherited	Boolean	True when the ACL permission is not set directly but inherited from an ancestor ACL object False if set directly on the ACL object
inherited_from_object	List[String]	The list of parent ACL object ids that contribute to inherited permission on an ACL object This is only defined if inherited is true

Object Types (object_type)

```
Currently: cluster, instance-pool, job, notebook, directory,
registered-model. In the future: experiments
```

FAQ

Where can I find object IDs?

- See How to get Workspace, Cluster, Notebook, and Job Details for where to find object ids.

Can we set permissions on all users?

- Yes, built in `users` group can be used to set permissions for all users.

Can I give someone the Can Manage permission on Jobs?

- The Can Manage permission is reserved for administrators. See Job permissions

How are Job cluster permissions configured?

- Clusters created during the run of a Job are initially configured using the permissions set on the Job:
  - Is Owner -> CAN_MANAGE
  - Can Manage Run -> CAN_MANAGE
  - Can View -> CAN_ATTACH_TO
- These permissions that are inherited from a Job will have inherited set to true, and contain the parent Job's ACL object_id in its inherited_from_object field in the form of /jobs/$jobId.
- If changes are made to a Job's permissions, any clusters created by that Job will also have those permissions.
- Permissions can also be set directly on the Jobs cluster using the clusters permissions API

Are there any directories which have some restrictions?

- **Root Directory:** The admins group by default has CAN_MANAGE permission on the root directory and this permission cannot be removed.
- **Home directory:** Each user has a designated home directory and the user by default has CAN_MANAGE permission on it which cannot be removed.
- **Trash and Shared directories:** Modifications to permissions on these directories is not allowed.