Further resources

In this document, you can:

1. See details of Azure Databricks access control for:

- Folders
- Notebooks
- Clusters
- Jobs

2. You can also link to extra detail on another feature that helps to secure critical Azure service resources - Azure VNet service endpoints.

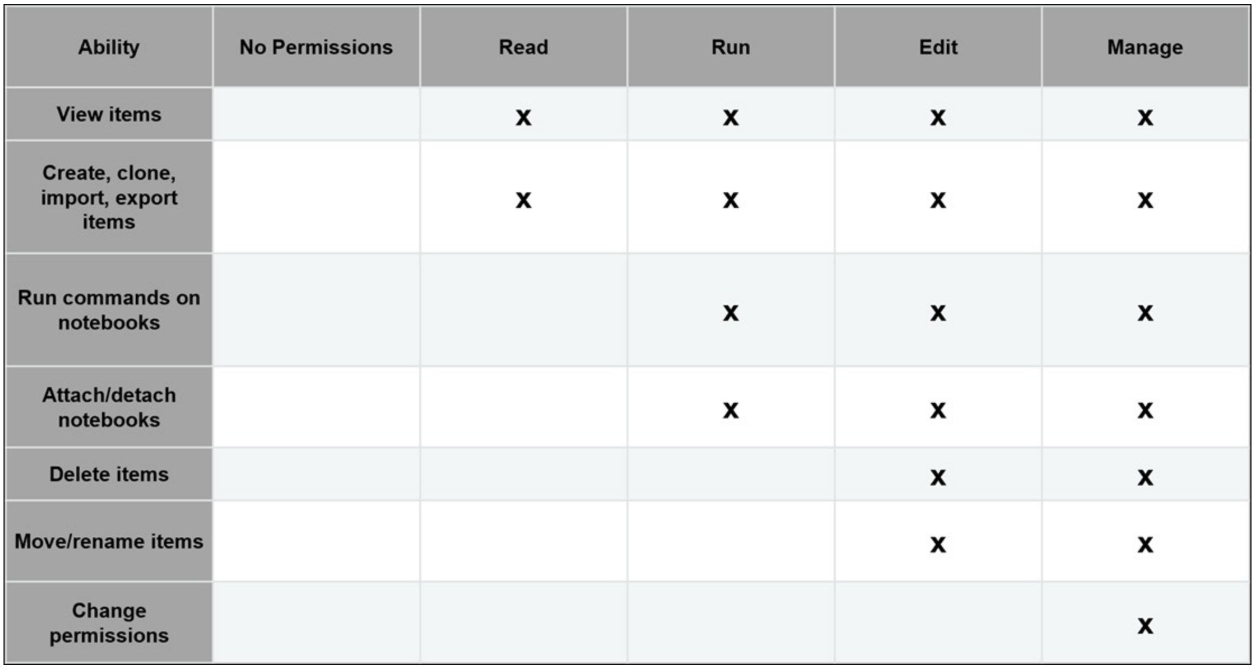
Access control - Folders

Access control is available only in the Premium SKU. By default, all users can create and modify workspace objects unless an administrator enables workspace access control.

You can assign five permission levels to notebooks and folders:

1. No Permissions,
2. Read,
3. Run,
4. Edit,
5. and Manage.

The following tables lists the abilities for each permission.

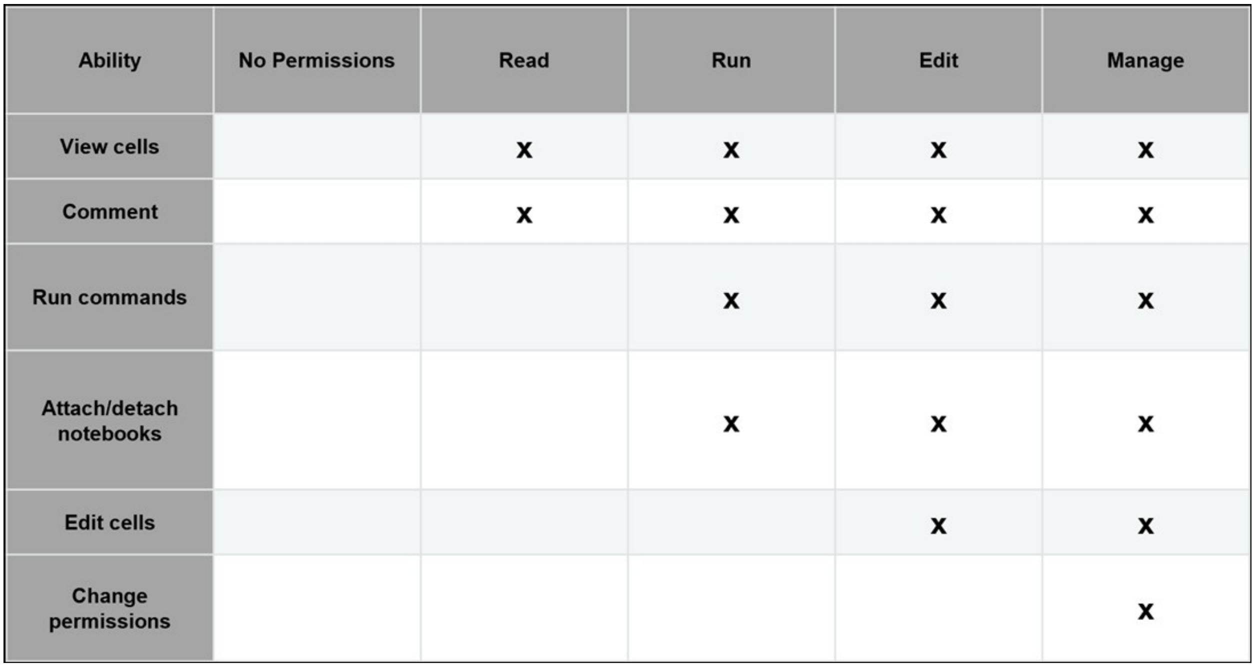


Ability	No Permissions	Read	Run	Edit	Manage
View items		x	x	x	x
Create, clone, import, export items		x	x	x	x
Run commands on notebooks			x	x	x
Attach/detach notebooks			x	x	x
Delete items				x	x
Move/rename items				x	x
Change permissions					x

Folder access control.

Access control - Notebooks

All notebooks in a folder inherit all permissions settings of that folder. For example, a user that has Run permission on a folder has Run permission on all notebooks in that folder.



Ability	No Permissions	Read	Run	Edit	Manage
View cells		x	x	x	x
Comment		x	x	x	x
Run commands			x	x	x
Attach/detach notebooks			x	x	x
Edit cells				x	x
Change permissions					x

Notebook access control.

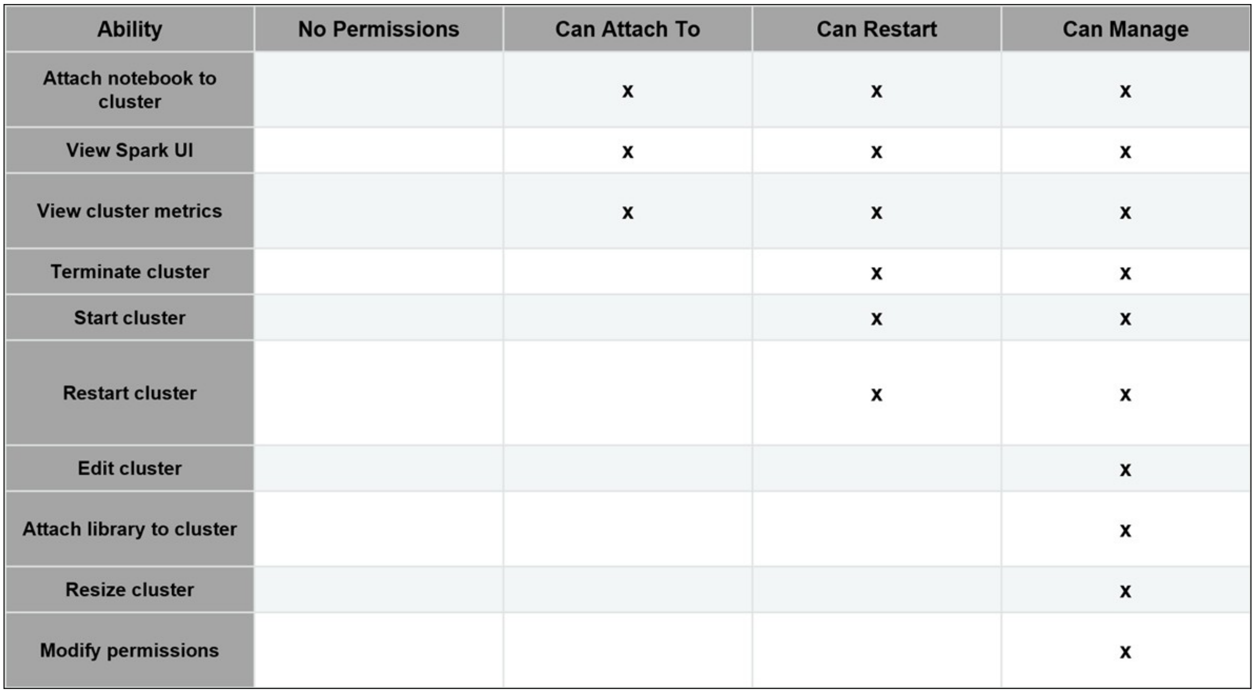
Access control - Clusters

All users can view libraries. To control who can attach libraries to clusters, manage access control on clusters.

There are four permission levels for a cluster:

1. No Permissions,
2. Can Attach To,
3. Can Restart,
4. and Can Manage

Note: *You have Can Manage permission for any cluster that you create*.



Ability	No Permissions	Can Attach To	Can Restart	Can Manage
Attach notebook to cluster		x	x	x
View Spark UI		x	x	x
View cluster metrics		x	x	x
Terminate cluster			x	x
Start cluster			x	x
Restart cluster			x	x
Edit cluster				x
Attach library to cluster				x
Resize cluster				x
Modify permissions				x

clusters access control.

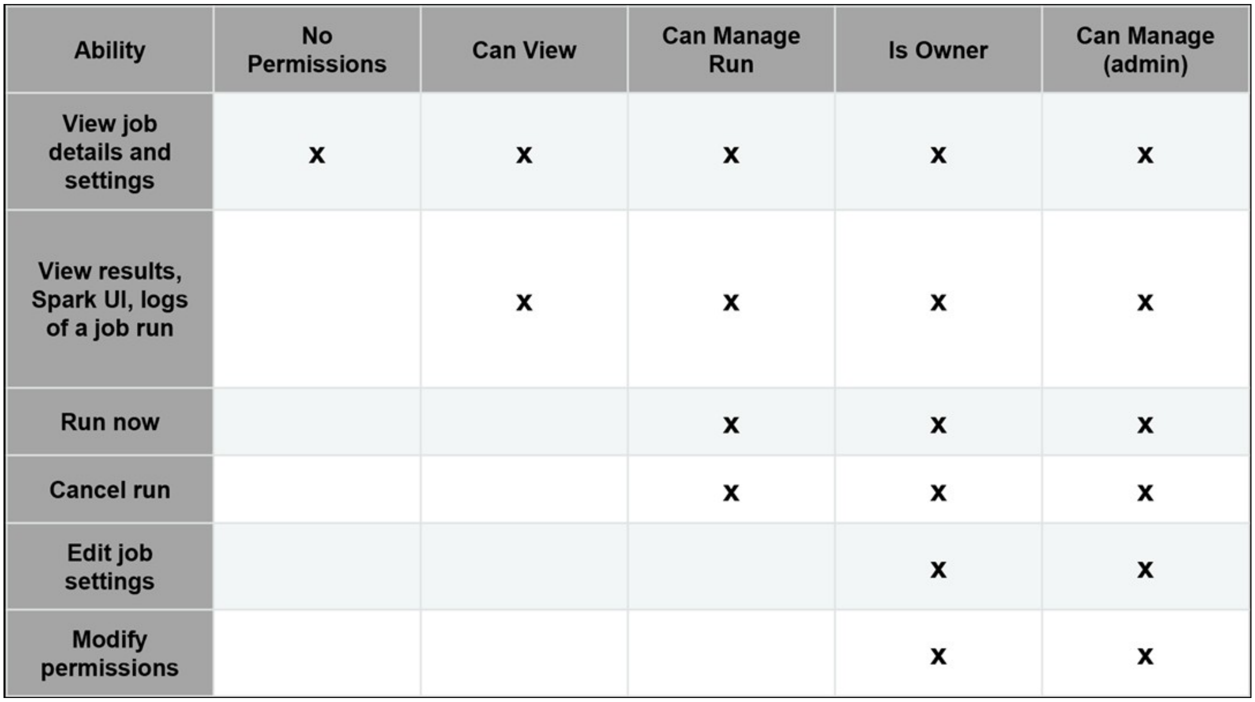
Access control - Jobs

To control who can run jobs and see the results of job runs, manage access control on jobs.

There are five permission levels for jobs:

1. No Permissions,
2. Can View,
3. Can Manage Run,
4. Is Owner,
5. and Can Manage.

Note: *The Can Manage permission is reserved for administrators.*



Ability	No Permissions	Can View	Can Manage Run	Is Owner	Can Manage (admin)
View job details and settings	x	x	x	x	x
View results, Spark UI, logs of a job run		x	x	x	x
Run now			x	x	x
Cancel run			x	x	x
Edit job settings				x	x
Modify permissions				x	x

Job access control.

Azure VNet service endpoints

Virtual Network (VNet) service endpoints extend your virtual network private address space. The endpoints also extend the identity of your VNet to the Azure services over a direct connection.

Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure network backbone.

Read more about securely accessing Azure data sources from Azure Databricks.