Comparing Log Analytics access modes

The following table summarizes the access modes:

	Workspace-centric	Resource-centric
Who is each model intended for?	Central administration. Administrators who need to configure data collection and users who need access to a wide variety of resources. Also currently required for users who have to access logs for resources outside of Azure.	Application teams. Administrators of Azure resources being monitored.
What does a user require to view logs?	Permissions to the workspace – builtin or custom Builtin Roles: Log Analytics Contributor Log Analytics Reader	Read access to the resource. Permissions can be inherited (i.e. from the containing resource group) or directly assigned to the resource. Permission to the logs for the resource will be automatically assigned.
What is the scope of permissions?	Workspace. Users with access to the workspace can query all logs in that workspace from tables that they hold permissions.	Azure resource. Users can query logs for resources they have access to from any workspace but can't query logs for other resources.
How can user access logs?	Start **Logs** from **Azure Monitor** menu or **Log Analytics workspaces**.	Start **Logs** from the menu for the Azure resource.