Understanding Roles & Permissions in Microsoft Sentinel

Microsoft Sentinel RBAC ensures least-privilege access and clear separation of duties.

PerparimLabs

© PerparimLabs | Cloud Security

Role Overview (Microsoft Docs Table)

- Sentinel includes 5 built-in roles for least-privilege access.
- roles table: Reader, Responder, Contributor, Playbook Operator, Automation Contributor.

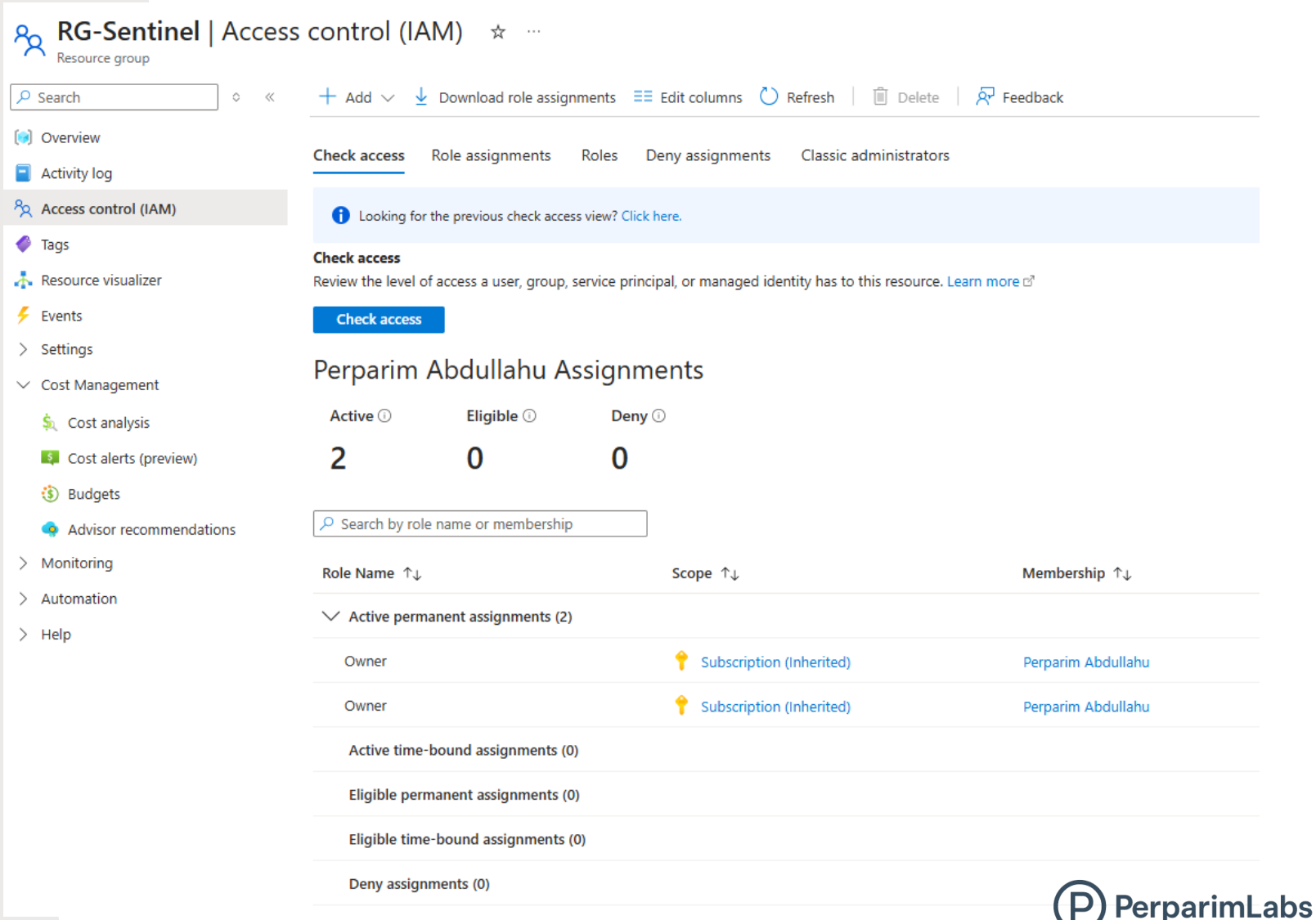
Role	SIEM support	Data lake support
Microsoft Sentinel Reader	View data, incidents, workbooks, and other resources	Access advanced analytics and run interactive queries on workspaces only.
Microsoft Sentinel Responder	All Reader permissions, plus manage incidents	N/A
Microsoft Sentinel Contributor	All Responder permissions, plus install/update solutions, create/edit resources	Access advanced analytics and run interactive queries on workspaces only.
Microsoft Sentinel Playbook Operator	List, view, and manually run playbooks	N/A
Microsoft Sentinel Automation Contributor	Allows Microsoft Sentinel to add playbooks to automation rules. Not used for user accounts.	N/A

PerparimLabs

© PerparimLabs | Cloud Security

IAM Overview

- Roles are managed via Access Control (IAM) in the resource group.
- RG-Sentinel Access Control IAM.

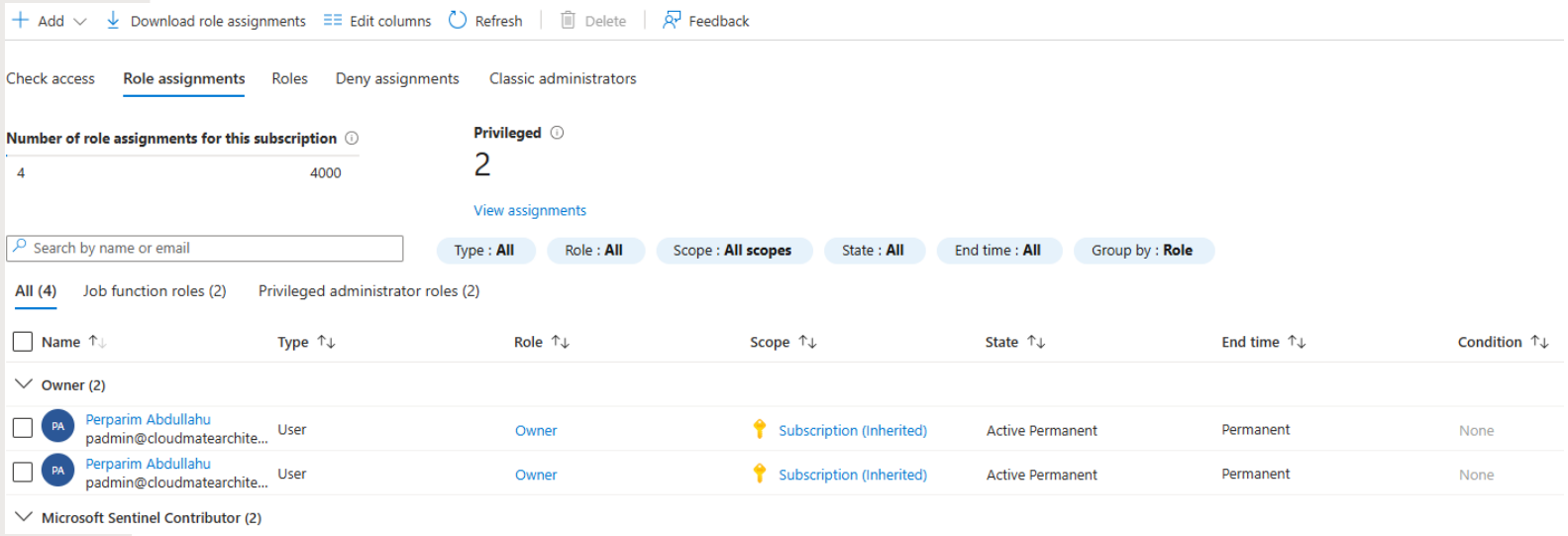


PerparimLabs

© PerparimLabs | Cloud Security

Current Assignments

- Azure RBAC Owner/Contributor may override Sentinel roles.
- role assignments list with Owner + Contributor.

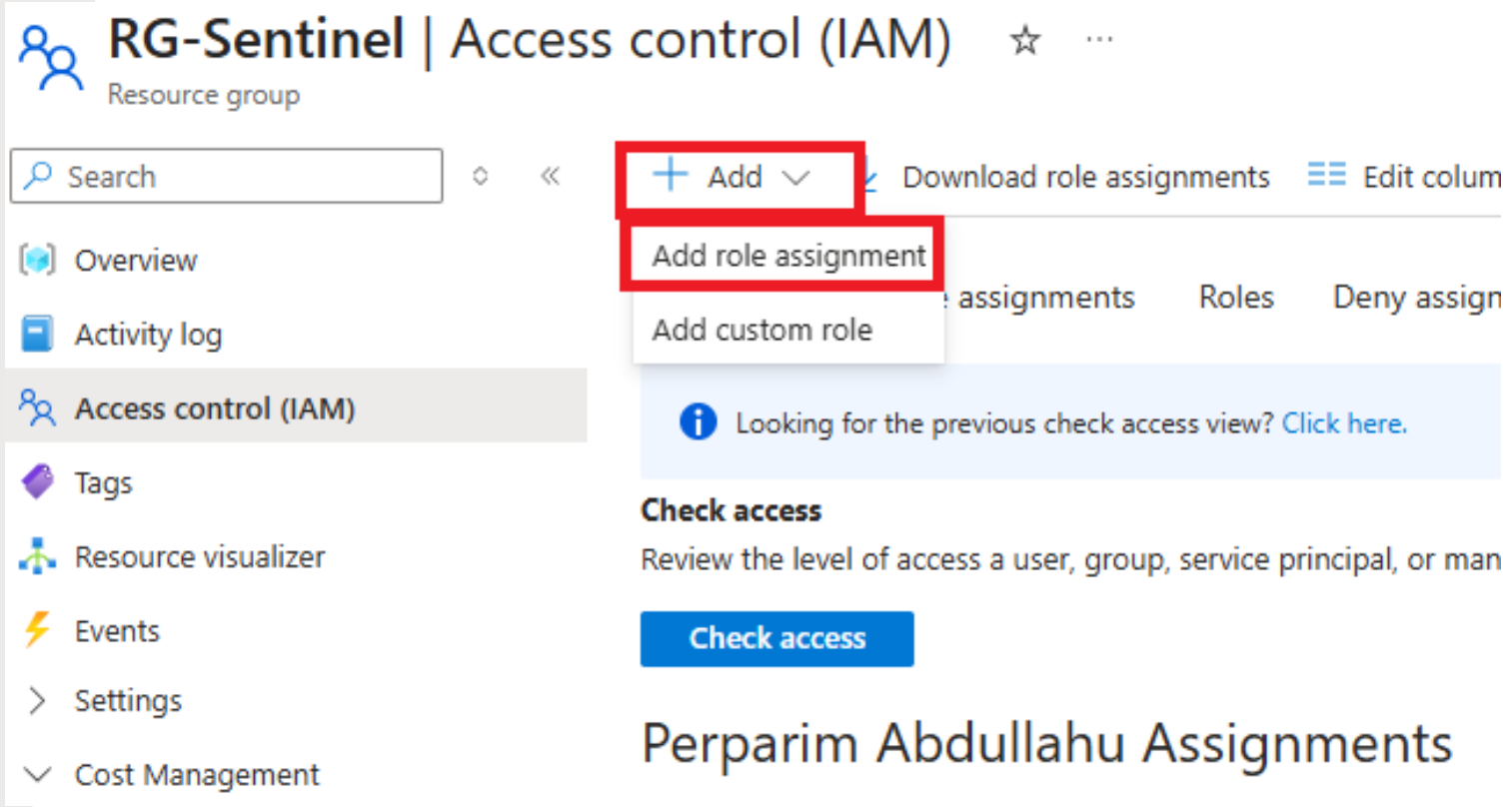


PerparimLabs

© PerparimLabs | Cloud Security

Add Role Assignment

- Assign Sentinel roles through IAM.
- Add → Role assignment.

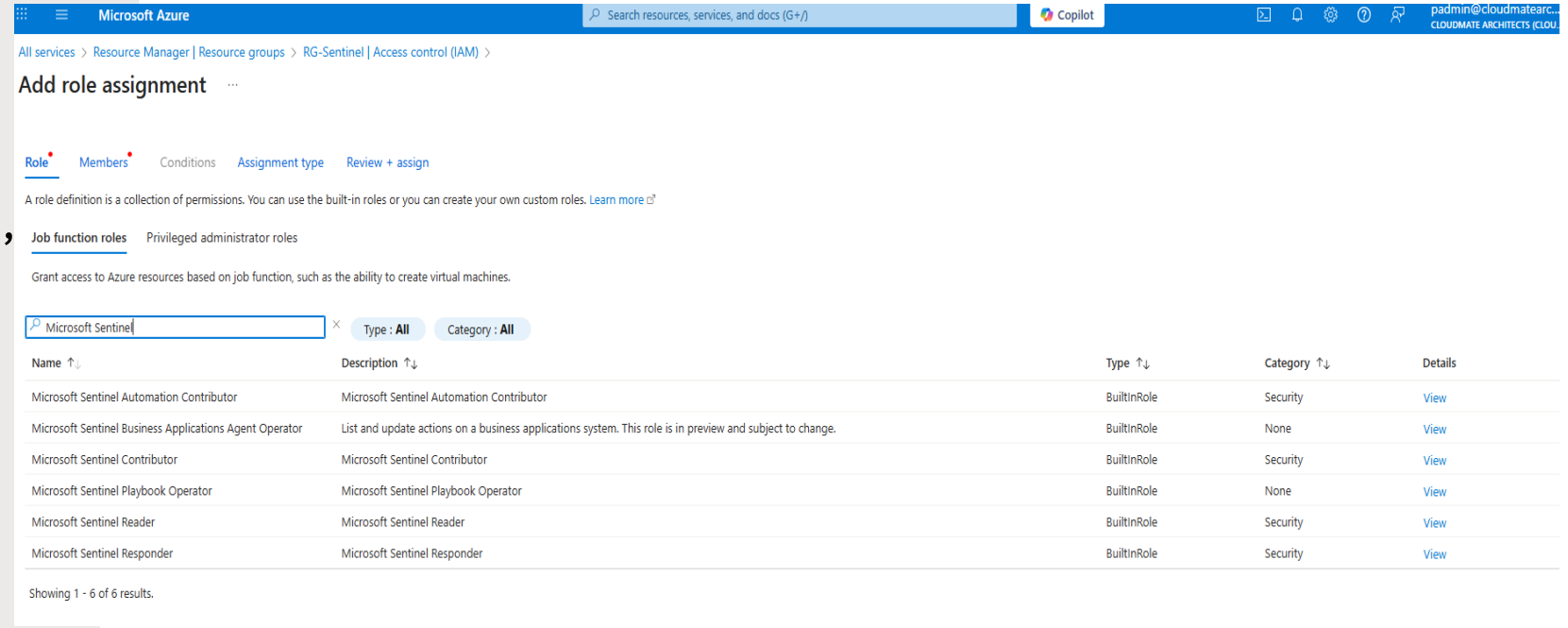


PerparimLabs

© PerparimLabs | Cloud Security

Filtering Sentinel Roles

- Filter to view all Sentinel roles available.
- search ‘Microsoft Sentinel’, roles appear.



PerparimLabs

© PerparimLabs | Cloud Security

Role Permissions Detail

- Each role grants specific actions. Example: Contributor can create rules and workbooks.
- *Sentinel Contributor permissions list.*

Microsoft Sentinel Contributor

BuiltInRole

Permissions JSON Assignments

Description: Microsoft Sentinel Contributor

Search permissions

Type : **All**

Permission Type

(•) Actions ( ) DataActions

Showing 500 of 1100 permissions View all (will take a moment to load)

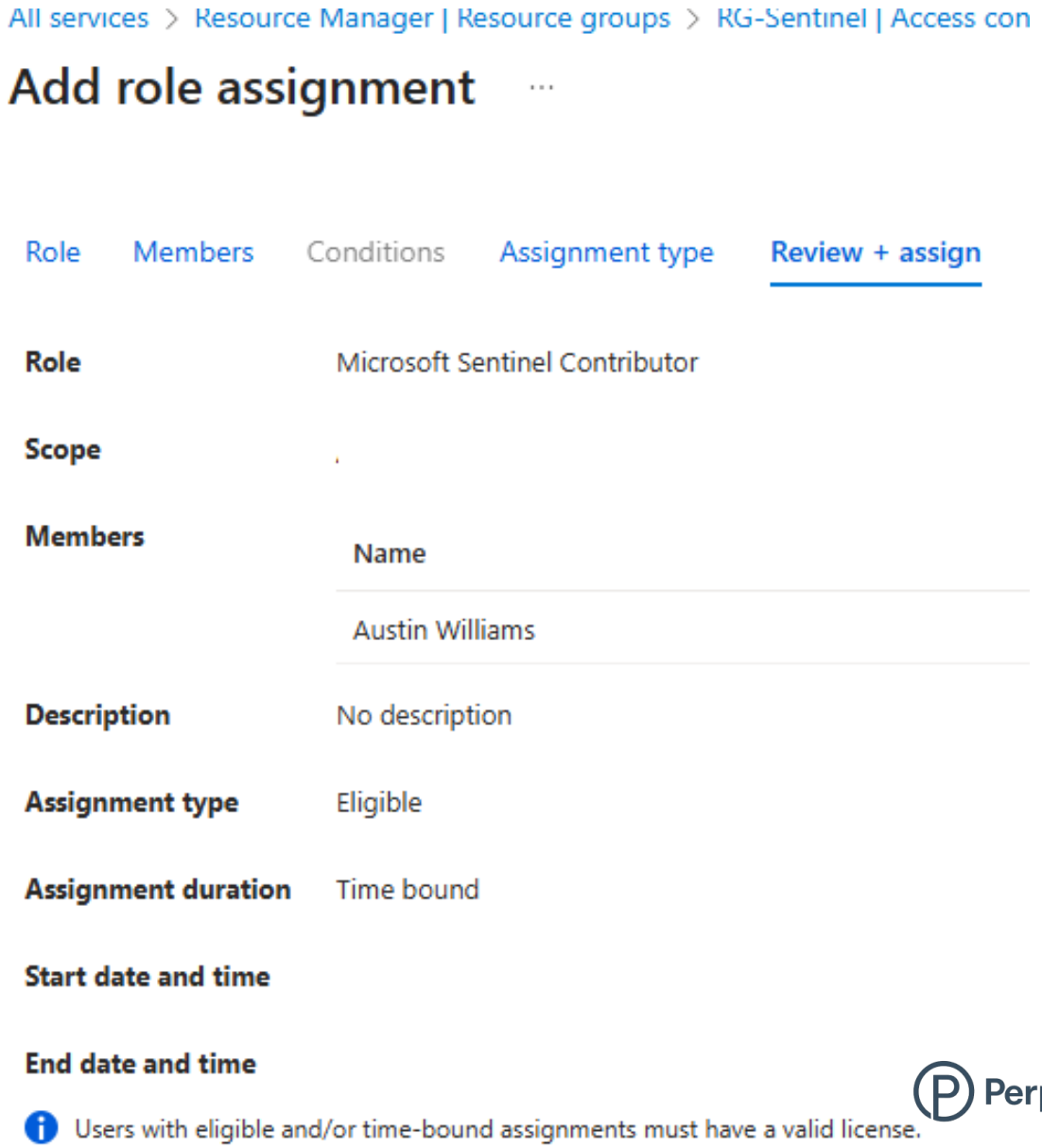
Type	Permissions	Description
Microsoft.Authorization		
Read	Acquire policy token operation	Acquire a policy token at the specified scope.
Read	Get administrator	Reads the administrators for the subscription.
Read	Get administrator operation statuses	Gets the administrator opreation statuses of the subscription.
Read	Get deny assignment	Get information about a deny assignment.
Read	Read the information about diagnostic settings categories	Get the information about diagnostic settings categories
Read	Get information about diagnostics settings	Read the information about diagnostics settings
Read	Get Role eligibility schedule instance	Gets the role eligibility schedule instances at given scope.
Read	Get management locks	Gets locks at the specified scope.
Read	Get operations	Gets the list of operations
Read	List permissions	Lists all the permissions the caller has at a given scope.
Read	Get policy assignment	Get information about a policy assignment.
Read	Get Private Link Association	Get information about private link association.
Read	Get Resource Management Private Link	Get information about resource management private link.
Read	Get Private Endpoint Connection	Get information about private endpoint connection.
Read	Get Private Endpoint Connection Proxy	Get information about private endpoint connection proxy.

PerparimLabs

© PerparimLabs | Cloud Security

Assigning to User

- Assign a role to a user or group with defined scope.
- Review + assign with member selected.

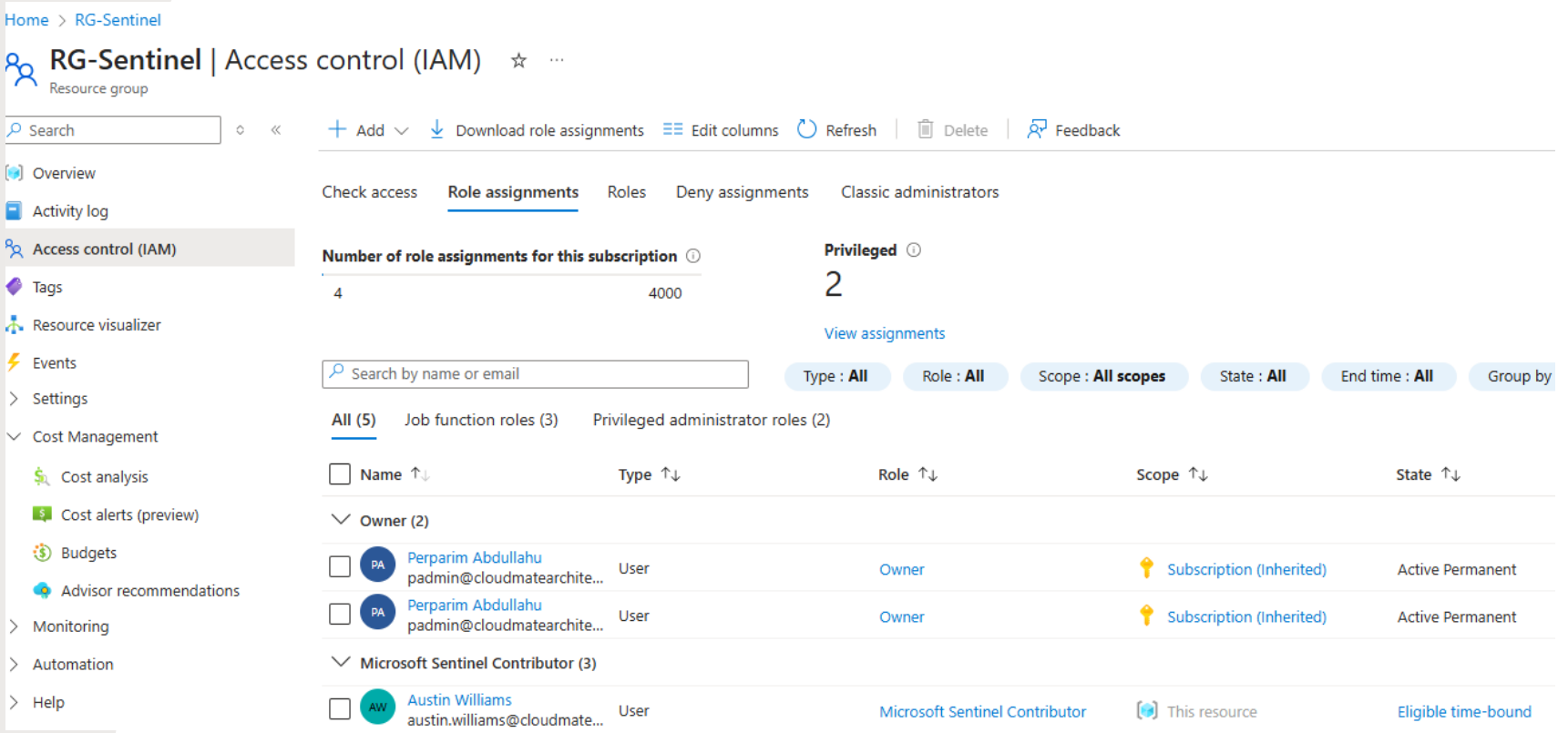


PerparimLabs

© PerparimLabs | Cloud Security

Confirmation

- Assignment confirmed. User now has Sentinel Contributor role.
- IAM showing Owner + Contributor + new user.



PerparimLabs

© PerparimLabs | Cloud Security

Key Takeaway

PerparimLabs

✔️ Reader = view only
✔️ Responder = manage incidents
✔️ Contributor = build & manage
✔️ Automation roles = playbooks & services”

© PerparimLabs | Cloud Security