

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	<i>None</i>
User9	Sydney	Owner

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Ambiente

Dominio contoso.com

Requerimientos técnicos

- Registra una aplicación llamada App2 en contoso.com
- Habilita Azure AD Privileged Identity Management (PIM) para contoso.com
- Habilita una directiva de acceso condicional para que cuando un usuario de cierto grupo no acceda desde su ciudad, suba su nivel de riesgo
- Siempre que sea posible, utilice el principio de privilegio mínimo

