Gestionarea subscriptions și a RBAC-ului

Introducere în laborator

În acest laborator, veți învăța despre controlul accesului bazat pe roluri. Veți învăța cum să utilizați permisiunile și domeniile de aplicare pentru a controla acțiunile pe care identitățile le pot și nu le pot efectua. De asemenea, veți învăța cum să simplificați gestionarea abonamentelor utilizând grupuri de gestionare.

Acest laborator necesită un abonament Azure. Tipul de abonament poate afecta disponibilitatea funcțiilor din acest laborator. Puteți schimba regiunea, dar pașii sunt scriși folosind **East US** .

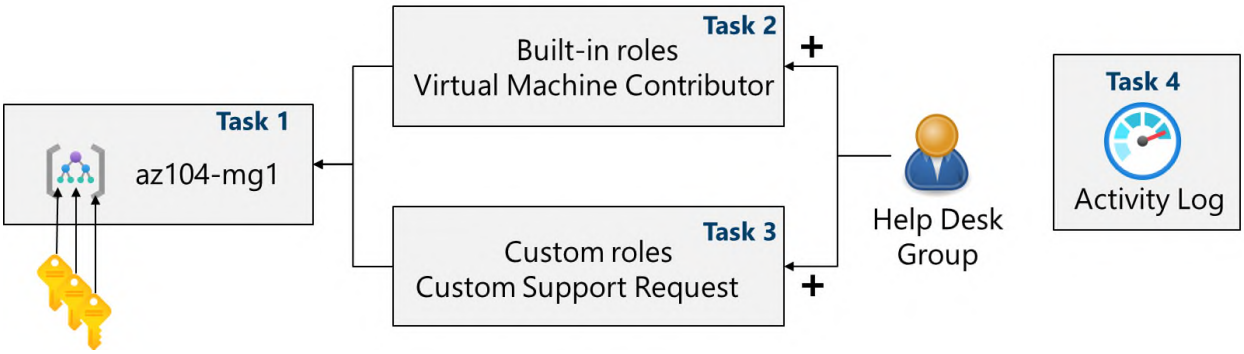
Timp estimat: 20 de minute

Scenariu de laborator

Pentru a simplifica gestionarea resurselor Azure în organizația dvs., vi s-a încredințat sarcina de a implementa următoarele funcționalități:

- Crearea unui grup de administrare care include toate abonamentele Azure.
- Acordarea permisiunilor de trimitere a solicitărilor de asistență pentru toate abonamentele din grupul de administrare. Permisiunile ar trebui să fie limitate doar la:
    - Creați și gestionați mașini virtuale
    - Creați tichete de solicitare de asistență (nu includeți adăugarea furnizorilor Azure)

Diagramă de arhitectură



Competențe profesionale

- Sarcina 1: Implementarea grupurilor de management.

- Sarcina 2: Examinați și atribuiți un rol Azure încorporat.
- Sarcina 3: Creați un rol RBAC personalizat.
- Sarcina 4: Monitorizați atribuirea rolurilor cu ajutorul Jurnalului de activități.

Sarcina 1: Implementarea grupurilor de management

În această sarcină, veți crea și configura grupuri de administrare. Grupurile de administrare sunt utilizate pentru a organiza și segmenta logic abonamentele. Acestea permit atribuirea și moștenirea RBAC și a politicilor Azure către alte grupuri de administrare și abonamente. De exemplu, dacă organizația dvs. are o echipă de asistență dedicată pentru Europa, puteți organiza abonamentele europene într-un grup de administrare pentru a oferi personalului de asistență acces la aceste abonamente (fără a oferi acces individual la toate abonamentele). În scenariul nostru, toți cei de la Biroul de asistență vor trebui să creeze o solicitare de asistență pentru toate abonamentele.

1. Conectați-vă la **portalul Azure** - https://portal.azure.com.
2. Căutați și selectați Microsoft Entra ID.
3. În lama **Gestionare** , selectați **Proprietăți** .
4. Consultați secțiunea **Gestionarea accesului pentru resursele Azure** . Observați/citiți că puteți gestiona accesul la toate abonamentele și grupurile de gestionare Azure din entitatea găzduită.
5. Căutați și selectați **Grupuri de gestionare** .
6. În lama **Grupuri de gestionare** , faceți clic pe **+ Creare** .
7. Creați un grup de administrare cu următoarele setări. Selectați **Trimitere** când ați terminat.

Setare	**Valoare**
ID-ul grupului de gestionare	az104-mg1(trebuie să fie unic în director)
Numele afișat al grupului de gestionare	az104-mg1

8. **Reîmprospătați** pagina grupului de administrare pentru a vă asigura că noul grup de administrare este afișat. Acest lucru poate dura un minut.

Notă: Ați observat grupul de gestionare rădăcină? Grupul de gestionare rădăcină este încorporat în ierarhie, astfel încât toate grupurile de gestionare și abonamentele să se adune în cadrul acestuia. Acest grup de gestionare rădăcină permite aplicarea politicilor globale și a atribuirilor de roluri Azure la nivel de director. După crearea unui grup de gestionare, veți adăuga orice abonamente care ar trebui incluse în grup.

Sarcina 2: Revizuirea și atribuirea unui rol Azure încorporat

În această sarcină, veți examina rolurile încorporate și veți atribui rolul de contribuitor VM unui membru al Biroului de asistență. Azure oferă un număr mare de roluri încorporate .

Notă: În pașii următori, veți atribui rolul grupului **de asistență tehnică** . Dacă nu aveți un grup de asistență tehnică, acordați-vă un minut pentru a-l crea.

1. Selectați grupul de gestionare **az104-mg1** .
2. Selectați blade-ul **Control acces (IAM)** , apoi fila **Roluri** .
3. Derulați prin definițiile de roluri încorporate care sunt disponibile. **Vizualizați** un rol pentru a obține informații detaliate despre **Permisiuni** , **JSON** și **Atribuiri** . Veți utiliza adesea *proprietățile „owner”* , *„contributor”* și *„reader”* .
4. Selectați **+ Adăugare** , din meniul derulant, selectați **Adăugare atribuire de rol** .
5. În lama **Adăugare atribuire rol** , căutați și selectați **Contribuitor mașină virtuală** . Rolul de contribuitor mașină virtuală vă permite să gestionați mașini virtuale, dar nu să accesați sistemul lor de operare sau să gestionați rețeaua virtuală și contul de stocare la care sunt conectate. Acesta este un rol bun pentru Biroul de asistență. Selectați **Următorul** .

Știați că... Azure oferea inițial doar modelul de implementare **clasic** . Acesta a fost înlocuit de modelul de implementare **Azure Resource Manager** . Ca practică recomandată, nu utilizați resurse clasice.

6. În fila **Membri** , **selectați Membri** .
7. Căutați și selectați helpdeskgrupul. Faceți clic pe **Selectare** .
8. Faceți clic de două ori **pe Revizuire + atribuire** pentru a crea atribuirea rolului.
9. Continuați pe blade-ul **Control acces (IAM)** . În fila **Atribuiri roluri** , confirmați că grupul **de asistență** are rolul **de Contribuitor mașină virtuală** .

Notă: Ca regulă generală, atribuiți întotdeauna roluri grupurilor, nu indivizilor.

Știați că...? Este posibil ca această atribuire să nu vă acorde privilegii suplimentare. Dacă aveți deja rolul de Proprietar, rolul respectiv include toate permisiunile asociate rolului de Contribuitor VM.

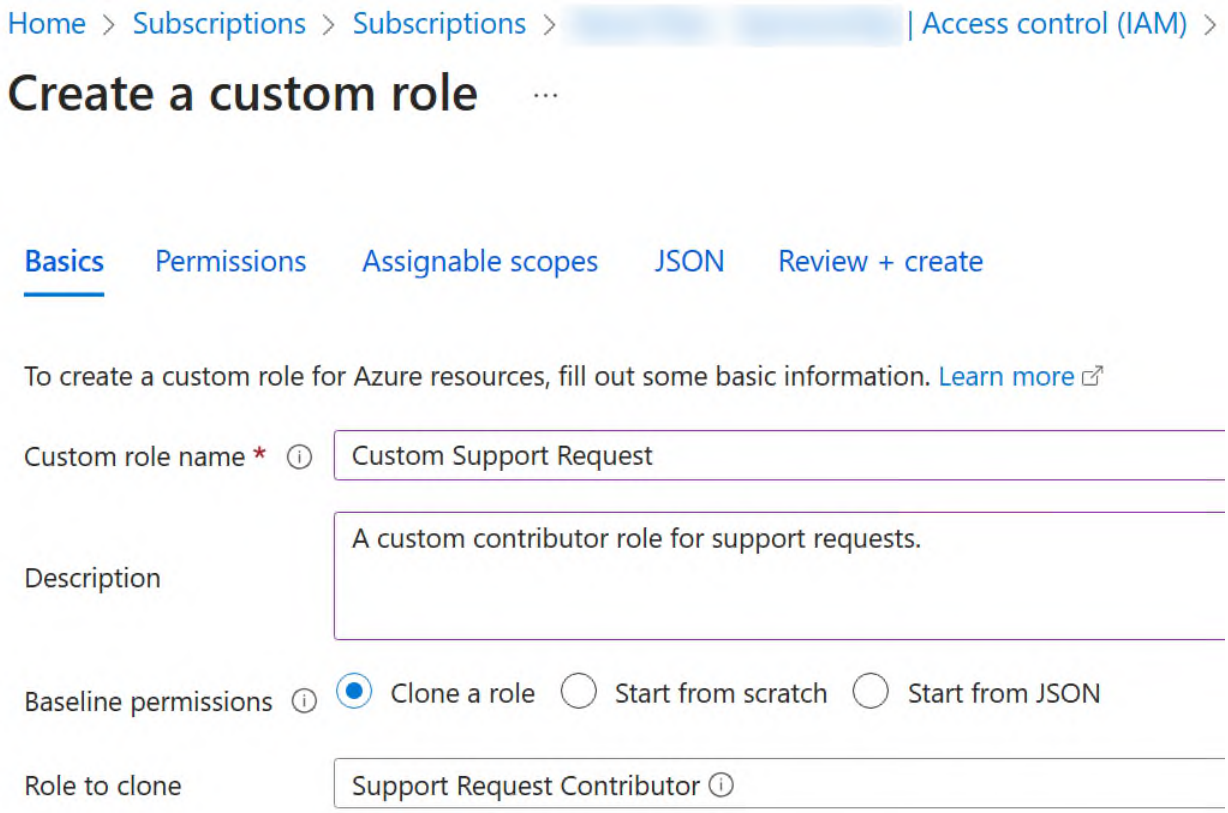
Sarcina 3: Creați un rol RBAC personalizat

În această sarcină, veți crea un rol RBAC personalizat. Rolurile personalizate sunt o parte esențială a implementării principiului privilegiilor minime pentru un mediu. Rolurile încorporate ar putea avea prea multe permisiuni pentru scenariul dvs. De asemenea, vom crea un rol nou și vom elimina permisiunile care nu sunt necesare. Aveți un plan pentru gestionarea permisiunilor care se suprapun?

1. Continuați să lucrați la grupul de administrare. Navigați la blade-ul **Control acces (IAM)** .
2. Selectați **+ Adăugare** , din meniul derulant, selectați **Adăugare rol personalizat** .
3. În fila Noțiuni de bază, finalizați configurația.

Setare	**Valoare**
Nume de rol personalizat	Custom Support Request
Descriere	A custom contributor role for support requests.

4. Pentru **Permisiuni de bază** , selectați **Clonează un rol** . În meniul derulant **Rol de clonat , selectați Contribuitor la cererea de asistență** .



5. Selectați **Următorul** pentru a trece la fila **Permisiuni** , apoi selectați **+ Excludeți permisiunile** .
6. În câmpul de căutare a furnizorului de resurse, introduceți .Supportși selectați **Microsoft.Support** .
7. În lista de permisiuni, bifați o casetă de selectare lângă **Altele: Înregistrează furnizorul de resurse de asistență** și apoi selectați **Adăugare** . Rolul ar trebui actualizat pentru a include această permisiune ca *NotAction* .

Notă: Un furnizor de resurse Azure este un set de operațiuni REST care activează funcționalitatea pentru un anumit serviciu Azure. Nu dorim ca Biroul de asistență să poată avea această capacitate, așa că este eliminată din rolul clonat.

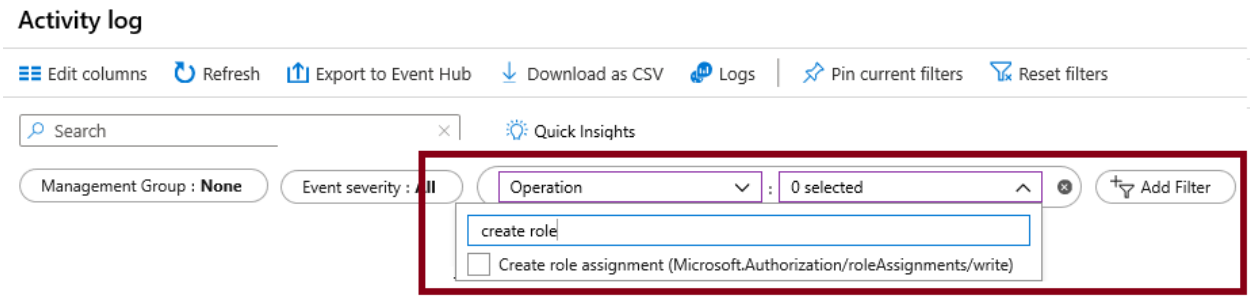
8. În fila **Domenii de aplicare atribuibile** , asigurați-vă că grupul de gestionare este listat, apoi faceți clic pe **Următorul** .
9. Revizuiți fișierul JSON pentru *Actions* , *NotActions* și *AssignableScopes* care sunt personalizate în rol.
10. Selectați **Revizuire + Creare** , apoi selectați **Creare** .

Notă: În acest moment, ați creat un rol personalizat și l-ați atribuit grupului de administrare.

Sarcina 4: Monitorizarea atribuirilor de roluri cu ajutorul Jurnalului de activități

În această sarcină, vizualizați jurnalul de activități pentru a determina dacă cineva a creat un rol nou.

1. În portal, localizați resursa **az104-mg1** și selectați **Jurnal de activitate** . Jurnalul de activitate oferă informații despre evenimentele la nivel de abonament.
2. Revizuiți activitățile pentru atribuirea rolurilor. Jurnalul de activități poate fi filtrat pentru operațiuni specifice.



Curățați-vă resursele

Dacă lucrați cu **propriul abonament,** acordați-vă un minut pentru a șterge resursele laboratorului. Acest lucru va asigura eliberarea resurselor și reducerea la minimum a costurilor. Cea mai ușoară modalitate de a șterge resursele laboratorului este să ștergeți grupul de resurse ale laboratorului.

- În portalul Azure, selectați grupul de administrare, selectați **Ștergere** și faceți clic pe **Da** pentru a confirma ștergerea.
- Folosind Azure PowerShell, Remove-AzManagementGroup -GroupName az104-mg1.
- Folosind interfața CLI, az account management-group delete --name az104-mg1.

Extinde-ți cunoștințele cu Copilot

Copilot vă poate ajuta să învățați cum să utilizați instrumentele de scriptare Azure. Copilot vă poate ajuta, de asemenea, în domenii care nu au fost abordate în laborator sau în care aveți nevoie de mai multe informații. Deschideți un browser Edge și alegeți Copilot (dreapta sus) sau navigați la *copilot.microsoft.com* . Acordați câteva minute pentru a încerca aceste solicitări.

- Creați două tabele care să evidențieze comenzile importante PowerShell și CLI pentru a obține informații despre abonamentele organizației pe Azure și explicați fiecare comandă în coloana „Explicații”.
- Care este formatul fișierului JSON Azure RBAC?
- Care sunt pașii de bază pentru crearea unui rol Azure RBAC personalizat?
- Care este diferența dintre rolurile Azure RBAC și rolurile Microsoft Entra ID?

Învață mai multe cu instruire în ritm propriu

- Securizați-vă resursele Azure cu controlul accesului bazat pe roluri Azure (Azure RBAC) . Utilizați Azure RBAC pentru a gestiona accesul la resurse în Azure.

Concluzii cheie

Felicitări pentru finalizarea laboratorului. Iată principalele concluzii ale acestui laborator.

- Grupurile de gestionare sunt utilizate pentru a organiza logic abonamentele.
- Grupul de gestionare rădăcină încorporat include toate grupurile de gestionare și abonamentele.
- Azure are multe roluri încorporate. Puteți atribui aceste roluri pentru a controla accesul la resurse.
- Puteți crea roluri noi sau puteți personaliza rolurile existente.
- Rolurile sunt definite într-un fișier formatat JSON și includ *Actions* , *NotActions* și *AssignableScopes* .
- Puteți utiliza Jurnalul de activități pentru a monitoriza atribuirea rolurilor.