

## Gestionarea identităților Microsoft Entra ID

### Introducere în laborator

Acesta este primul dintr-o serie de laboratoare pentru administratorii Azure. În acest laborator, veți învăța despre utilizatori și grupuri. Utilizatorii și grupurile sunt elementele de bază ale unei soluții de identitate.

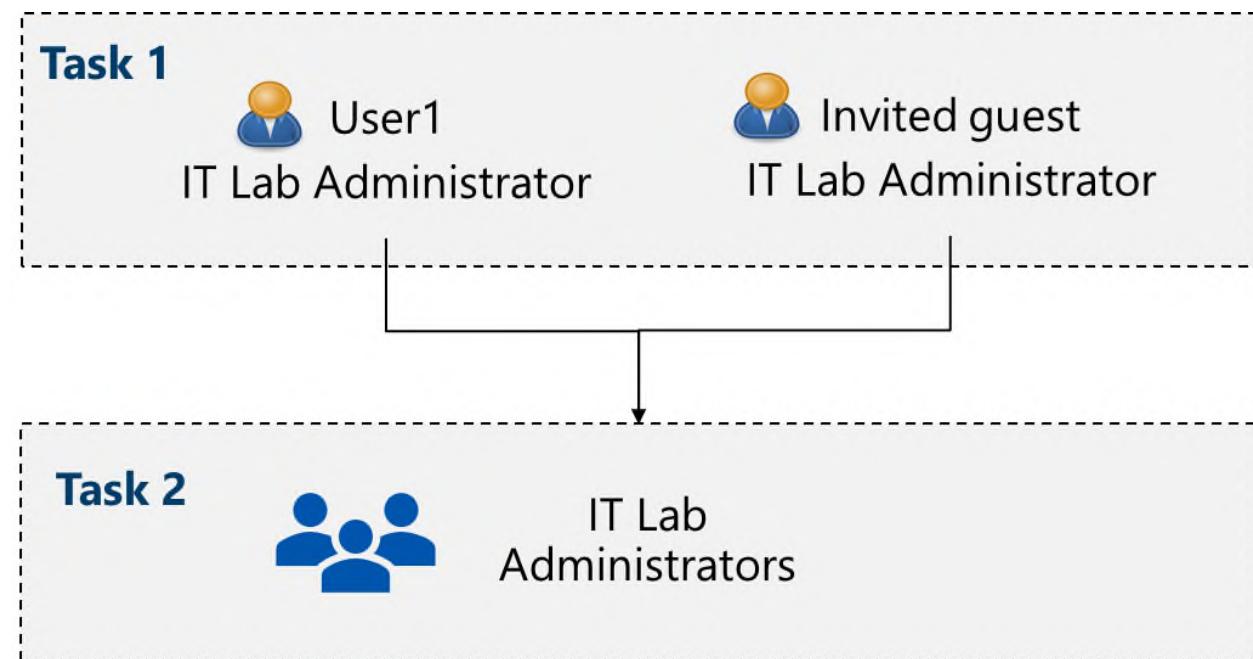
Acest laborator necesită un abonament Azure. Tipul de abonament poate afecta disponibilitatea funcțiilor din acest laborator. Puteți schimba regiunea, dar pașii sunt scriși folosind **East US**.

**Timp estimat: 30 de minute**

### Scenariu de laborator

Organizația dumneavoastră construiește un nou mediu de laborator pentru testarea în pre-producție a aplicațiilor și serviciilor. Sunt angajați câțiva ingineri pentru a gestiona mediul de laborator, inclusiv mașinile virtuale. Pentru a permite inginerilor să se autentifice utilizând Microsoft Entra ID, vi s-a încredințat sarcina de a furniza utilizatori și grupuri. Pentru a minimiza cheltuielile administrative, apartenența la grupuri ar trebui actualizată automat pe baza titlurilor posturilor.

### Diagramă de arhitectură



### Competențe profesionale

- Sarcina 1: Crearea și configurarea conturilor de utilizator.

- Sarcina 2: Creați grupuri și adăugați membri.

### Sarcina 1: Crearea și configurarea conturilor de utilizator

În această sarcină, veți crea și configura conturi de utilizator. Conturile de utilizator vor stoca date despre utilizatori, cum ar fi numele, departamentul, locația și informațiile de contact.

1. Conectați-vă la **portalul Azure** - <https://portal.azure.com>.
2. Pentru a continua la portal, selectați **Anulare** pe ecranul de pornire **Bun venit în Azure**.

**Notă:** Portalul Azure este utilizat în toate laboratoarele. Dacă sunteți nou în Azure, căutați și selectați Quickstart Center. Acordați câteva minute pentru a viziona videoclipul **Introducere în portalul Azure**. Chiar dacă ați mai utilizat portalul înainte, veți găsi câteva sfaturi și trucuri despre navigarea și personalizarea interfeței.

3. Căutați și selectați Microsoft Entra ID. Microsoft Entra ID este soluția de gestionare a identității și accesului bazată pe cloud de la Azure. Acordați-vă câteva minute pentru a vă familiariza cu unele dintre caracteristicile listate în panoul din stânga.
4. Selectați lama **Prezentare generală**, apoi fila **Gestionare chiriași**.

**Știați că...?** O entitate găzduită este o instanță specifică a Microsoft Entra ID care conține conturi și grupuri. În funcție de situația dvs., puteți crea mai multe entități găzduite și **puteți comuta** între ele.

5. Reveniți la pagina **Introduceți ID** apăsând tasta **Înapoi** în browser sau selectând opțiunea din meniul de navigare.
6. Pe măsură ce aveți timp, explorați alte opțiuni, cum ar fi **Licențe** și **Resetare parolă**.

### Creați un utilizator nou

1. În lama **Gestionare**, selectați **Utilizatori**; apoi, în meniul derulant **Utilizator nou**, selectați **Creare utilizator nou**.
2. Creați un utilizator nou cu următoarele setări (lăsați-i pe ceilalți cu setările implicite). În fila **Proprietăți**, observați toate tipurile diferite de informații care pot fi incluse în contul de utilizator.

<b>Setare</b>	<b>Valoare</b>
Numele principal al utilizatorului	az104-user1
Numele de afişare	az104-user1
Generare automată parolă	<b>verificat</b>
Cont activat	<b>verificat</b>
Titlul postului (fila Proprietăți)	IT Lab Administrator
Departament (fila Proprietăți)	IT
Locația de utilizare (fila Proprietăți)	<b>Statele Unite</b>

3. După ce ați terminat de revizuit, selectați **Revizuire + creare** și apoi **Creare**.
4. Reîmprospătați pagina și confirmați că noul utilizator a fost creat.

#### **Invitați un utilizator extern**

1. În meniul derulant **Utilizator nou**, selectați **Invitați un utilizator extern**.

<b>Setare</b>	<b>Valoare</b>
E-mail	Adresa dvs. de e-mail
Numele de afişare	Numele dumneavoastră
Trimite mesaj de invitație	<b>bifați căsuța</b>
Mesaj	Welcome to Azure and our group project

2. Accesați fila **Proprietăți**. Completați informațiile de bază, inclusiv aceste câmpuri.

<b>Setare</b>	<b>Valoare</b>
Denumirea funcției	IT Lab Administrator

<b>Setare</b>	<b>Valoare</b>
Departament	IT
Locația de utilizare (fila Proprietăți)	<b>Statele Unite</b>

3. Selectați **Recenzie + invitație**, apoi **Invită**.
4. **Reîmprospătați** pagina și confirmați că utilizatorul invitat a fost creat. Ar trebui să primiți în scurt timp e-mailul de invitație.

**Notă:** Este puțin probabil să creați conturi de utilizator individual. Știți cum intenționează organizația dvs. să creeze și să gestioneze conturile de utilizator?

### Sarcina 2: Crearea de grupuri și adăugarea de membri

În această sarcină, creați un cont de grup. Conturile de grup pot include conturi de utilizator sau dispozitive. Există două moduri de bază în care membrii sunt atribuiți grupurilor: static și dinamic. Grupurile statice necesită ca administratorii să adauge și să eliminate manual membri. Grupurile dinamice se actualizează automat pe baza proprietăților unui cont de utilizator sau dispozitiv. De exemplu, funcția.

1. În portalul Azure, căutați și selectați Microsoft Entra ID. În lama **Gestionare**, selectați **Grupuri**.
2. Acordați-vă un minut pentru a vă familiariza cu setările de grup din panoul din stânga.
  - **Expirarea** vă permite să configurați durata de viață a grupului în zile. După acest interval, grupul trebuie reînnoit de către proprietar.
  - **Politica de denumire** vă permite să configurați cuvinte blocate și să adăugați un prefix sau un sufix la numele grupurilor.
3. În lama **Toate grupurile**, selectați + **Grup nou** și creați un grup nou.

<b>Setare</b>	<b>Valoare</b>
Tipul grupului	<b>Securitate</b>
Numele grupului	IT Lab Administrators

Setare	Valoare
Descrierea grupului	Administrators that manage the IT lab
Tipul de membru	<b>Atribuit</b>

4. **Notă :** Pentru abonamentul dinamic este necesară o licență Entra ID Premium P1 sau P2. Dacă sunt disponibile și alte **tipuri de abonament**, opțiunile vor apărea în meniul derulant.

[Home](#) > [Groups](#) > [Groups](#) | All groups >

## New Group ...

 Got feedback?

---

Group type \* ⓘ  
 ▼

Group name \* ⓘ  
 ✓

Group description ⓘ  
 ✓

Microsoft Entra roles can be assigned to the group ⓘ  
 Yes    No

Membership type \* ⓘ

▼

Owners

[No owners selected](#)

Members

5. [No members selected](#)

6. Selectați **Niciun proprietar selectat**.

7. În pagina **Adăugare proprietari**, căutați și **selectați** -vă (afișat în colțul din dreapta sus) ca proprietar. Observați că puteți avea mai mult de un proprietar.

8. Selectați **Niciun membru selectat**.

9. În panoul **Adăugare membri**, căutați și **selectați** az104 -**user1** și **utilizatorul invitat**. Adăugați ambii utilizatori la grup.

10. Selectați **Creare** pentru a implementa grupul.

11. **Reîmprospătați** pagina și asigurați-vă că grupul a fost creat.

12. Selectați noul grup și examinați informațiile despre **Membri** și **Proprietari**.

**Notă:** Este posibil să gestionați un număr mare de grupuri. Organizația dvs. are un plan pentru crearea de grupuri și adăugarea de membri?

### **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 alegeti Copilot (dreapta sus) sau navigați la [copilot.microsoft.com](https://copilot.microsoft.com). Acordați câteva minute pentru a încerca aceste solicitări.

- Care sunt comenzi Azure PowerShell și CLI pentru a crea un grup de securitate numit Administratori IT? Furnizați pagina oficială de referință a comenziilor.
- Oferiți o strategie pas cu pas pentru gestionarea utilizatorilor și grupurilor în Microsoft Entra ID.
- Care sunt pașii din portalul Azure pentru a crea în bloc utilizatori și grupuri?
- Furnizați un tabel comparativ al conturilor de utilizator Microsoft Entra ID interne și externe.

### **Învață mai multe cu instruire în ritm propriu**

- [Întelgește Microsoft Entra ID](#). Comparați Microsoft Entra ID cu Active Directory DS, aflați despre Microsoft Entra ID P1 și P2 și explorați Microsoft Entra Domain Services pentru gestionarea dispozitivelor și aplicațiilor asociate domeniului în cloud.
- [Creați utilizatori și grupuri Azure în Microsoft Entra ID](#). Creați utilizatori în Microsoft Entra ID. Întelgeți diferite tipuri de grupuri. Creați un grup și adăugați membri. Gestionăți conturile de oaspete business-to-business.
- [Permiteți utilizatorilor să își reseteze parola cu resetarea parolei în regim self-service în Microsoft Entra](#). Evaluăți resetarea parolei în regim self-service pentru a permite utilizatorilor din organizația dvs. să își reseteze parolele sau să își

deblocheze conturile. Configurați, configurați și testați resetarea parolei în regim self-service.

### **Concluzii cheie**

Felicitări pentru finalizarea laboratorului. Iată câteva dintre principalele aspecte ale acestui laborator:

- O entitate găzduită reprezintă organizația dvs. și vă ajută să gestionați o instanță specifică a serviciilor cloud Microsoft pentru utilizatorii dvs. interni și externi.
- ID-ul Microsoft Entra are conturi de utilizator și de oaspete. Fiecare cont are un nivel de acces specific domeniului de activitate care se așteaptă să fie efectuat.
- Grupurile combină utilizatori sau dispozitive corelate. Există două tipuri de grupuri, inclusiv Securitate și Microsoft 365.
- Apartenența la grup poate fi atribuită static sau dinamic.