

*OBS: For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.*

Lab scenario

You have been asked to create a proof of concept showing how Azure users and groups are created. Also, how role-based access control is used to assign roles to groups. Specifically, you need to:

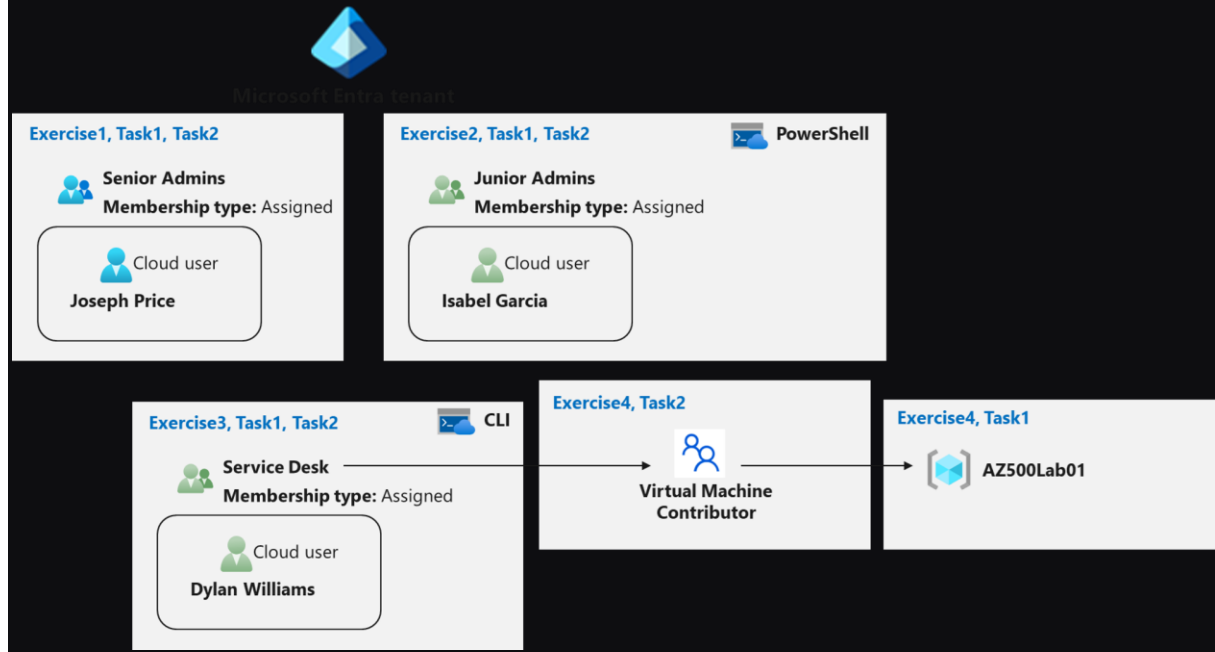
- Create a Senior Admins group containing the user account of Joseph Price as its member.
- Create a Junior Admins group containing the user account of Isabel Garcia as its member.
- Create a Service Desk group containing the user account of Dylan Williams as its member.
- Assign the Virtual Machine Contributor role to the Service Desk group.

Lab objectives

In this lab, you will complete the following exercises:

- Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).
- Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).
- Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).
- Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

Role-Based Access Control architecture diagram



Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member.

Painel > Diretório Padrão | Usuários > Usuários

Joseph Price


Usuário


Pesquisar x < Editar propriedades Excluir Atualizar Redefinir senha Revogar sessões Gerenciar exibição Algum comentário?

- Visão geral
- Logs de auditoria
- Logs de entrada
- Diagnosticar e resolver problemas
- Atributos de segurança personalizados
- Funções atribuídas
- Unidades administrativas
- Grupos
- Aplicativos
- Licenças
- Dispositivos
- Atribuições de função do Azure
- Métodos de autenticação
- Nova solicitação de suporte

Visão geral Monitoramento Propriedades


Informações básicas


 **Joseph Price**
joseph-price@davirocha2014hotmail.onmicrosoft.com
Member




Nome UPN	joseph-price@davirocha2014hotmail.onmicrosoft.com	Associações de grupo	1
ID do objeto	0aa24390-9707-4320-be2a-d80400f5c32e	Aplicativos	0
Data e hora de criação	4 de fev. de 2026, 09:29	Funções atribuídas	0
Tipo de usuário	Membro	Licenças atribuídas	0
Identities	davirocha2014hotmail.onmicrosoft.com		

Meu Feed

 **Status da conta**
● Habilitado
[Editar](#)

 **Convite de colaboração B2B**
[Converter em usuário externo](#)

Ações rápidas

 [Editar propriedades](#)

Painel > Diretório Padrão | Usuários > Usuários > Joseph Price | Grupos > Senior Admins

Senior Admins | Membros

Grupo

+ Adicionar membros Operações em massa Atualizar Gerenciar a exibição Remover Algum comentário?

- Visão geral
- Diagnosticar e resolver problemas
- Gerenciar
 - Propriedades
 - Membros**
 - Proprietários
 - Funções e administradores
 - Unidades administrativas
 - Associações a um grupo
 - Aplicativos
 - Licenças
 - Atribuições de função do Azure
- Atividade
 - Privileged Identity Management
 - Revisões de acesso
 - Logs de auditoria
 - Resultados da operação em massa
- Solução de Problemas e Suporte

Membros diretos Todos os membros

Pesquisar Adicionar filtro

1 membro do grupo encontrado

<input type="checkbox"/>	Nome	Tipo	Email	Tipo de usuário	ID do objeto	ID do dispositi...
<input type="checkbox"/>	Joseph Price	Usuário		Membro	0aa24390-9707-4320-be2a-d80400f5c32e	

Exercise 2: Create a Junior Admins group containing the user account of Isabel Garcia as its member.

```
Alternar para Bash  Reiniciar  Gerenciar arquivos  Nova sessão  Editor  Visualização da Web  Configurações  Ajuda  Solicitando um Cloud Shell.Succeeded. Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: Share your feedback and help us improve Cloud Shell: https://aka.ms/cloudshell/feedback

VERBOSE: Authenticating to Azure ...
PS /home/davi> $passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
PS /home/davi> $passwordProfile.Password = "Pa55w.rd1234"
PS /home/davi> Connect-AzureAD
PS /home/davi> $domainName = ((Get-AzureADTenantDetail).VerifiedDomains)[0].Name
PS /home/davi> New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'

ObjectID                DisplayName              UserPrincipalName        UserType
-----
fc6c555-8770-467d-a553-f27194782cae Isabel Garcia Isabel@davirocha2014hotmail.onmicrosoft.com Member

PS /home/davi> Get-AzureADUser -All $true | Where-Object {$_.UserPrincipalName -like "Isabel@lab.LabInstance.Id*"}
PS /home/davi> New-AzureADGroup -DisplayName 'Junior Admins@lab.LabInstance.Id' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins

ObjectID                DisplayName              Description
-----
4470c26e-cde8-45f6-9872-9dad23d5c642 Junior Admins@lab.LabInstance.Id

PS /home/davi> Get-AzureADGroup

ObjectID                DisplayName              Description
-----
4470c26e-cde8-45f6-9872-9dad23d5c642 Junior Admins@lab.LabInstance.Id
6bc18aa6-65f9-42de-8cd4-50a09b2e8ad0 Senior Admins

PS /home/davi> $user = Get-AzureADUser -Filter "UserPrincipalName eq 'isabel@davirocha2014hotmail.onmicrosoft.com'"
PS /home/davi> Add-AzADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins@lab.LabInstance.Id"
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.
PS /home/davi> Get-AzADGroupMember -GroupDisplayName "Junior Admins@lab.LabInstance.Id"

AccountEnabled          : True
AgeGroup                :
ApproximateLastSignInDateTime :
BusinessPhone           : {}
City                    :
CompanyName              :
ComplianceExpirationDateTime :
ConsentProvidedForMinor :
Country                 :
CreatedDateTime          : 2/4/2026 1:37:56 PM
CreationType             :
DeletedDateTime          :
Department              :
DeviceVersion            :
DisplayName              : Isabel Garcia
EmployeeHireDate         :
EmployeeId               :
EmployeeOrgData          : {
}
EmployeeType             :
ExternalUserState        :
ExternalUserStateChangeDateTime :
FaxNumber                :
GivenName                :
Id                       : fc6c555-8770-467d-a553-f27194782cae
Identity                 : {{
  "issuer": "davirocha2014hotmail.onmicrosoft.com",
  "issuerAssignedId": "Isabel@davirocha2014hotmail.onmicrosoft.com",
  "signInType": "userPrincipalName"
}}
InAddress                : {}
IsResourceAccount        :
JobTitle                 :
LastPasswordChangeDateTime :
LegalAgeGroupClassification :
LegalAgeGroupClassification :
Mail                    :
MailNickName             : Isabel
Manager                  : {
}
MobilePhone              :
OdataId                  :
OdataType                 : #microsoft.graph.user
OfficeLocation            :
OnPremisesImmutableId    :
OnPremisesLastSyncDateTime :
OnPremisesSyncEnabled    :
OperatingSystem           :
OperatingSystemVersion   :
OtherMail                 : {}
PasswordPolicy            :
PasswordProfile           : {
  "forceChangePasswordNextSignIn": true,
  "forceChangePasswordNextSignInWithMfa": false
}
PhysicalId               :
PostalCode               :
PreferredLanguage         :
ProxyAddress              : {}
ResourceGroupName        :
ShowInAddressList         :
SignInSessionsValidFromDateTime : 2/4/2026 1:37:56 PM
State                    :
StreetAddress             :
Surname                   :
TrustType                 :
UsageLocation             :
UserPrincipalName         : Isabel@davirocha2014hotmail.onmicrosoft.com
UserType                  : Member
AdditionalProperties       : [[@odata.type, #microsoft.graph.user], [id, fc6c555-8770-467d-a553-f27194782cae], [accountEnabled, True], [businessPhones, System.Object[]]]

PS /home/davi> 
```

Exercise 3: Create a Service Desk group containing the user account of Dylan Williams as its member.

```
Solicitando um Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
davi [ ~ ]$ az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\\/\\\\/'
davi [ ~ ]$ az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "businessPhones": [],
  "displayName": "Dylan Williams",
  "givenName": null,
  "id": "3f60145d-288f-48bf-bf11-114250fab89e",
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "Dylan@davirocha2014hotmail.onmicrosoft.com"
}
davi [ ~ ]$ az ad user list --output table
-----
DisplayName      GivenName  PreferredLanguage  Surname  UserPrincipalName
-----
Davi Rocha       Davi       en                 Rocha    davirocha2014_hotmail.com#EXT#@davirocha2014hotmail.onmicrosoft.com
Dylan Williams
Isabel Garcia
Joseph Price     Joseph
davi [ ~ ]$ az ad group create --display-name "Service Desk" --mail-nickname "ServiceDesk"
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#groups/$entity",
  "classification": null,
  "createdDateTime": "2026-02-04T16:37:06Z",
  "creationOptions": [],
  "deletedDateTime": null,
  "description": null,
  "displayName": "Service Desk",
  "expirationDateTime": null,
  "groupTypes": [],
  "id": "b7cb15a6-dcd7-43b1-9848-f4b4971cabf6",
  "isAssignableToRole": null,
  "mail": null,
  "mail": null,
  "mailEnabled": false,
  "mailNickname": "ServiceDesk",
  "membershipRule": null,
  "membershipRuleProcessingState": null,
  "onPremisesDomainName": null,
  "onPremisesLastSyncDateTime": null,
  "onPremisesMetadata": null,
  "onPremisesProvisioningErrors": [],
  "onPremisesSecurityIdentifier": null,
  "onPremisesSyncEnabled": null,
  "preferredDataLocation": null,
  "preferredLanguage": null,
  "proxyAddresses": [],
  "renewalDateTime": "2026-02-04T16:37:06Z",
  "resourceBehaviorOptions": [],
  "resourceProvisioningOptions": [],
  "securityEnabled": true,
  "securityIdentifier": "S-1-12-1-3003539878-1135729879-3035908248-4138409111",
  "serviceProvisioningErrors": [],
  "theme": null,
  "uniqueName": null,
  "visibility": null
}
davi [ ~ ]$ az ad group list -o table
-----
CreatedDateTime  DisplayName  NullEnabled  MailNickname  RenewalDateTime  SecurityEnabled  SecurityIdentifier
-----
2026-02-04T13:38:57Z  JuniorAdmins  False       JuniorAdmins  2026-02-04T13:38:57Z  True            S-1-12-1-1148240494-1173802472-2912776856-1120326947
2026-02-04T12:31:00Z  SeniorAdmins  False       SeniorAdmins  2026-02-04T12:31:00Z  True            S-1-12-1-1807846854-1121871353-2689651852-3498716827
2026-02-04T16:37:06Z  ServiceDesk  False       ServiceDesk   2026-02-04T16:37:06Z  True            S-1-12-1-3003539878-1135729879-3035908248-4138409111
davi [ ~ ]$ az ad user show \
--id Dylan@davirocha2014hotmail.onmicrosoft.com \
-o json | jq -r '.id'
davi [ ~ ]$ az ad group member add --group "Service Desk" --member-id $OBJECTID
davi [ ~ ]$ az ad group member list --group "Service Desk"
{
  "@odata.type": "microsoft.graph.user",
  "businessPhones": [],
  "displayName": "Dylan Williams",
  "givenName": null,
  "id": "3f60145d-288f-48bf-bf11-114250fab89e",
  "jobTitle": null,
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "Dylan@davirocha2014hotmail.onmicrosoft.com"
}
]
davi [ ~ ]$
```

Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group

Pesquisar recursos, serviços e documentos (G+)

Copilot

📧

davirocha2014@hotmail...

DIRETÓRIO PADRÃO (DAVIROCH...

AZ500Lab01

Grupo de recursos

Gerar código Bicep para duplicar este grupo de recursos

Exportar grupos de recursos usando Bicep ou Terraform +1

Pesquisar

«

+ Criar

Gerenciar a exibição

Excluir o grupo de recursos

Renovar

Exportar para CSV

Consulta aberta

...

Agrupar por nenhum

Visão geral

Log de atividade

IAM (Controle de acesso)

Marcações

Visualizador de recursos

Eventos

Configurações

Gerenciamento de Custos

Monitoramento

Automação

Ajuda

Fundamentos

Assinatura (mover) : Assinatura do Azure 1

Implantações : Nenhuma implantação

ID da Assinatura : 62e77354-db9b-4f24-9235-1c0ba46a574c

Localização : East US

Rótulos (editar) : Adicionar marcas

Recursos

Recomendações

Filtrar por qualquer ca...

Tipo é igual a tudo

Localização é igual a tudo

+ Adicionar filtro

Nenhum recurso corresponde aos seus filtros

Experimente alterar ou limpar seus filtros.

+ Criar

Limpar filtros

Saiba mais

Mostrando 1 - 0 de 0. Contagem de exibição: au...

Enviar comentários

Painel > Resource Manager | Grupos de Recursos > AZ500Lab01 | IAM (Controle de acesso)

Adicionar atribuição de função

Função

Membros

Condições

Examinar + atribuir

Uma definição de função é uma coleção de permissões. Você pode usar as funções internas ou criar suas próprias funções personalizadas. Saiba mais

O Copilot pode ajudar a escolher uma função

Funções de trabalho

Funções de administrador privilegiadas

Conceda acesso aos recursos do Azure com base na função de trabalho, como a capacidade de criar máquinas virtuais.

virtual machine contributor

Tipo: Todos

Categoria: Todos

Nome ↑	Descrição ↑	Tipo ↑	Categoria ↑	Detalhes
Desktop Virtualization Power On Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start virtual machines.	BuiltInRole	Nenhum	Exibir
Desktop Virtualization Power On Off Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start and stop virtual machines.	BuiltInRole	Nenhum	Exibir
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to create, delete, update, start, and stop virt...	BuiltInRole	Nenhum	Exibir
Service Fabric Cluster Contributor	Manage your Service Fabric Cluster resources. Includes clusters, application types, application type versions, applications, and services. You will need additio...	BuiltInRole	Nenhum	Exibir

Mostrando 1 - 4 de 4 resultados.

Painel

Resource Manager | Grupos de Recursos

AZ500Lab01 | IAM (Controle de acesso)

Pesquisar recursos, serviços e documentos (G+)

Copilot

...

Adicionar atribuição de função

...

×

Função

Membros

Condições

Examinar + atribuir

Função selecionada

Desktop Virtualization Virtual Machine Contributor

Atribuir acesso a

Usuário, grupo ou entidade de serviço

Identidade gerenciada

Membros

+ Selecionar membros

Nome	ID de objeto	Tipo
Service Desk	b7cb15a6-dcd7-43b1-9848-44b4971cabf6	Grupo

Description

Optional

Painel

Resource Manager | Grupos de Recursos

AZ500Lab01

Pesquisar recursos, serviços e documentos (G+)

Copilot

davirocha2014@hotmail...
desenvolvimento guavoca...

AZ500Lab01 | IAM (Controle de acesso)

...

×

Pesquisar

«

+ Adicionar

↕ Baixar as atribuições de função

≡ Editar colunas

🔄 Atualizar

🗑 Excluir

💬 Comentários

Visão geral

Log de atividade

IAM (Controle de acesso)

Marcações

Visualizador de recursos

Eventos

Configurações

Gerenciamento de Custos

Monitoramento

Automação

Ajuda

Verificar acesso

Atribuições de função

Funções

Atribuições de negação

Administradores clássicos

Número de atribuições de função desta assinatura

2

4000

Privilegiado

1

Exibir tarefas

Pesquisar por nome ou email

Tipo: Todos

Função: Todos



Escopo: Todos os escopos

Agrupar por: Função

Todos (2)

Funções de trabalho (1)

Funções de administrador privilegiadas (1)

Nome ↑↓	Tipo ↑↓	Função ↑↓	Escopo ↑↓	Condição ↑↓
> Proprietário (1)				
▼ Desktop Virtualization Virtual Machine Contributor (1)				
<input type="checkbox"/>  Service Desk b7cb15a6-dcd7-43b1-9848-44b4971cabf6	Grupo	Desktop Virtualization Virtual Machine Contribu...	 Este recurso	Nenhum

Mostrando 1 - 2 de 2 resultados.

Dylan Williams atribuições – AZ500Lab01

×

Atribuições de função atuais

Atribuições qualificadas

As atribuições para o usuário, o grupo, a entidade de serviço ou a identidade gerenciada selecionada nesse escopo ou herdada pelo escopo.

Pesquisar por nome da atribuição ou descrição

Atribuições de função (1)

Função	Descrição	Escopo	Atribuição de grupo	Condição
Desktop Virtualization Vi	This role is in preview and subjec...	Este recurso	Service Desk	Nenhum

Atribuições de negação (0)

Administradores clássicos (0)