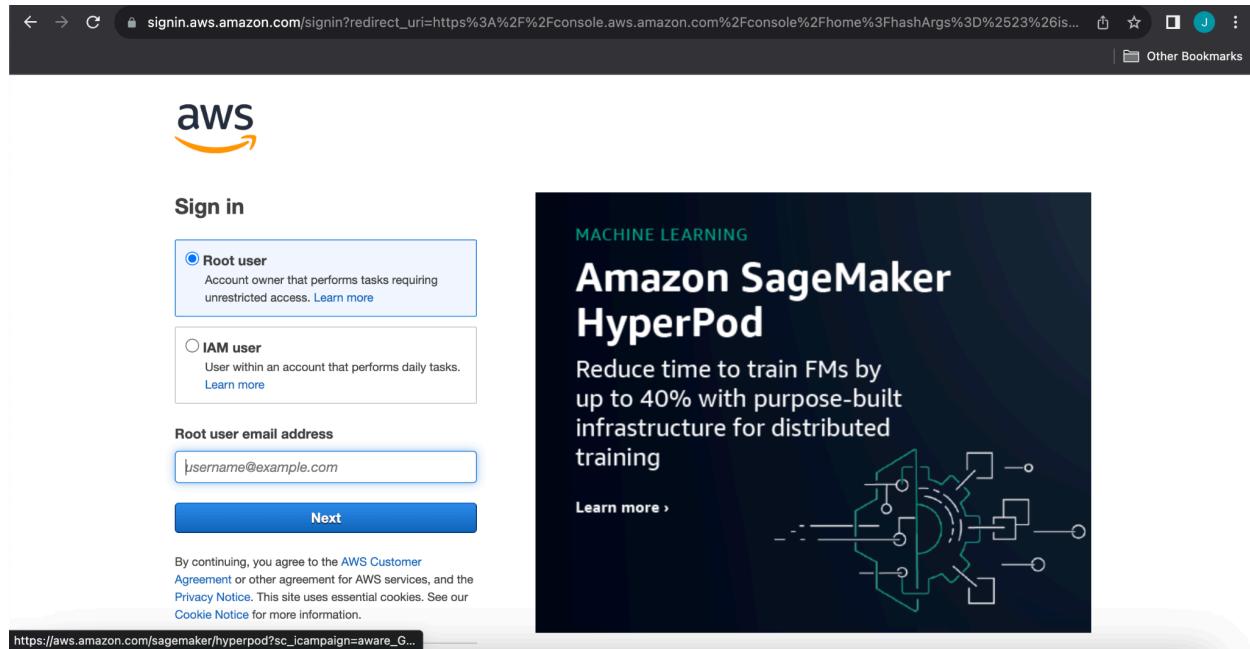
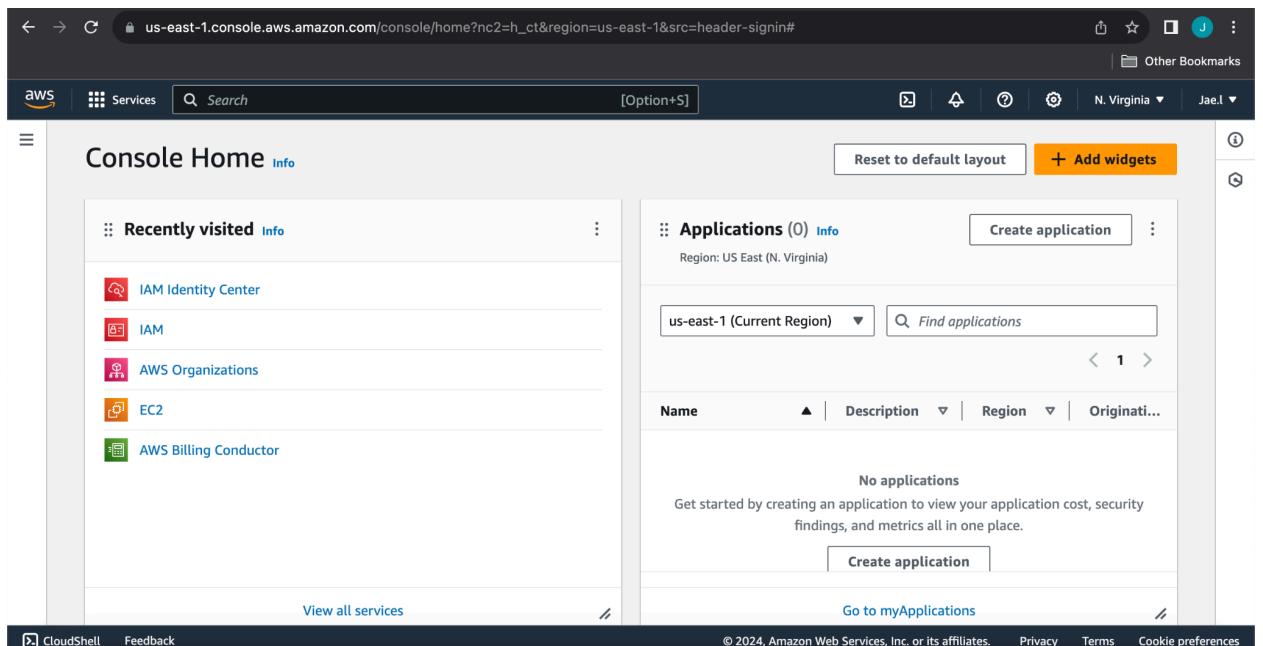


● Creating Users, User Groups and Permissions

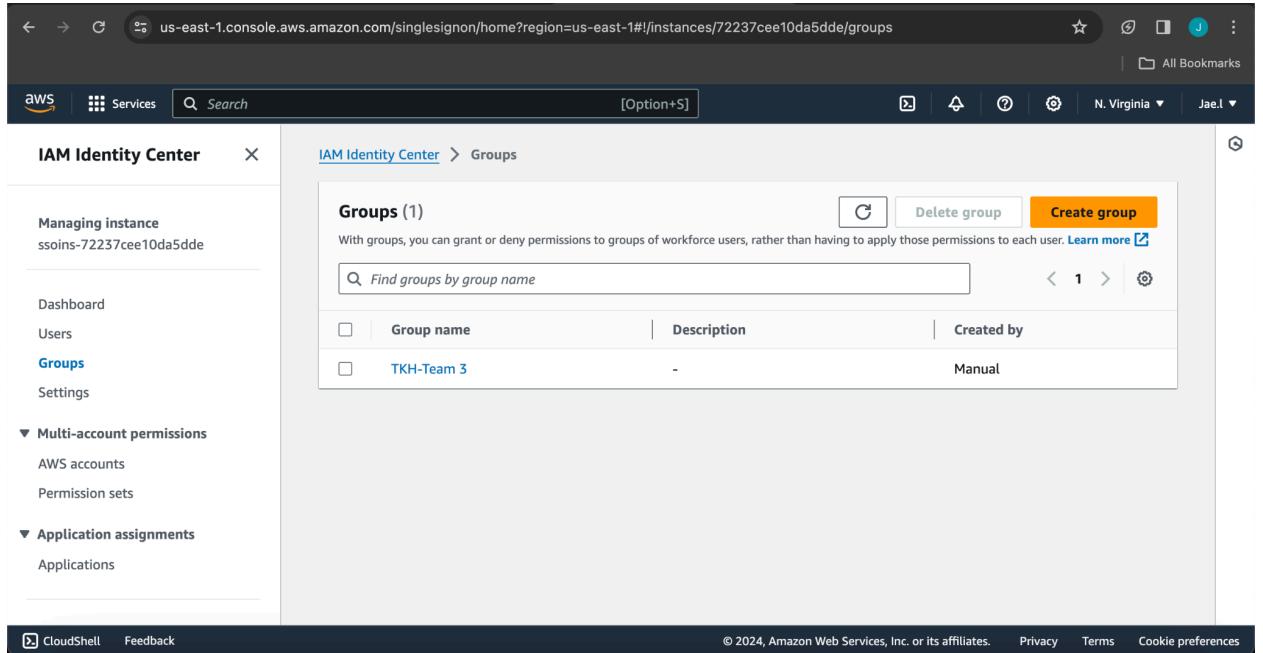
1. When creating IAM user and user groups, sign in as the root user.



2. In search bar you can type “IAM Identity Center”, proceed to the link

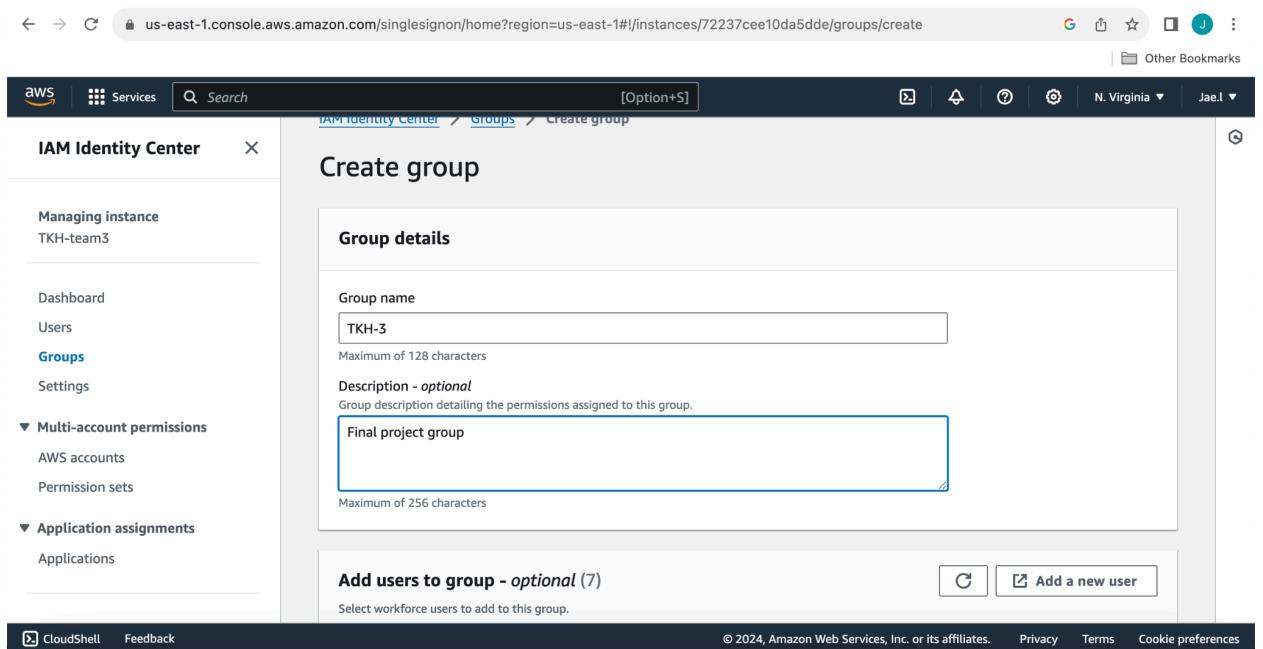


3. Go to > User Groups > Create group



The screenshot shows the AWS IAM Identity Center Groups page. On the left, there's a sidebar with options like Dashboard, Users, Groups (which is selected and highlighted in blue), Settings, Multi-account permissions, AWS accounts, and Permission sets. Below these are Application assignments and Applications. The main content area shows a table titled "Groups (1)". The table has columns for Group name, Description, and Created by. There is one entry: "TKH-Team 3" with a description of "-" and created by "Manual". At the top right of the table are buttons for "Delete group" and "Create group" (which is highlighted in orange). Above the table, there's a note: "With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)". A search bar at the top says "Find groups by group name". The bottom of the page includes standard AWS footer links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

4. Input a group name and description > Create group



The screenshot shows the "Create group" page. The sidebar on the left is identical to the previous screenshot. The main area is titled "Create group" and contains a "Group details" section. It has two fields: "Group name" (containing "TKH-3") and "Description - optional" (containing "Final project group"). Below this is an "Add users to group - optional (7)" section with a note: "Select workforce users to add to this group." At the bottom right of this section is a button for "Add a new user". The bottom of the page includes standard AWS footer links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

- We will now add user “Raven” to our group named TKH-3
5. Go to Users > Add User

The screenshot shows the AWS IAM Identity Center interface. On the left, there's a sidebar with navigation links like Dashboard, Users, Groups, Settings, Multi-account permissions, AWS accounts, Permission sets, and Application assignments. The main area is titled "Users (7)" and lists seven users with their details: Edgardo-TKH, Takala-TKH, Awa-TKH, Giovanni-TKH, Jaelin-TKH, Jasmine-TKH, and Jesus-TKH. Each user has a checkbox next to their name, and columns for Display name, Status (Enabled), MFA devices (1 device or None), and Created by (Manual). At the top right, there are buttons for "Delete users" and "Add user". The bottom of the screen includes standard AWS footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

6. Input user credentials, include a user email to invite them to the project.

This screenshot shows the "Add User Wizard" step 1: "User details". The left sidebar is identical to the previous screenshot. The main form contains fields for generating a one-time password (unchecked), Email address (ravenem145@yahoo.com), Confirm email address (ravenem145@yahoo.com), First name (Raven), Last name (Nahem), and Display name (Raven Nahem). Below the display name field is a note: "This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list." At the bottom, there's a section for "Contact methods - optional". The bottom of the screen includes standard AWS footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

7. Click > Next

The screenshot shows the 'Add user' wizard in the AWS IAM Identity Center. The left sidebar shows 'Managing instance' set to 'TKH-team3'. The main area is titled 'Specify user details' and contains five optional sections: 'Contact methods - optional', 'Job-related information - optional', 'Address - optional', 'Preferences - optional', and 'Additional attributes - optional'. At the bottom right of the main area is a yellow 'Next' button.

8. Add user to a group > Next

The screenshot shows the 'Add user' wizard in the AWS IAM Identity Center, Step 2: 'Add user to groups'. The left sidebar shows 'Managing instance' set to 'TKH-team3'. The main area shows 'Step 1: Specify user details' completed and 'Step 2 - optional: Add user to groups' selected. Below it is 'Step 3: Review and add user'. On the right, a 'Groups (1/1)' section lists 'TKH-Team 3' with a checkbox checked. A yellow 'Next' button is at the bottom right.

9. Click > Add user

The screenshot shows the AWS IAM Identity Center interface. On the left, a sidebar lists navigation options: Dashboard, Users (which is selected), Groups, Settings, Multi-account permissions (AWS accounts, Permission sets), and Application assignments (Applications). The main content area is titled "Step 2: Add user to groups - optional". It displays a table titled "Groups (1)" with one item: "TKH-Team 3". The table has columns for "Group name" and "Description". At the bottom right of the table are buttons for "Cancel", "Previous", and "Add user". Above the table, there are two sections: "Preferences - optional" and "Additional attributes - optional". The top of the screen shows the URL "us-east-1.console.aws.amazon.com/singlesignon/home?region=us-east-1#/instances/72237cee10da5dde/users\$addUserWizard" and the AWS logo.

10. User successfully created

The screenshot shows the AWS IAM Identity Center interface after a user has been successfully added. A green success message at the top states: "The user "Raven-TKH" was successfully added. The user will receive an email with a link to set up a password and instructions to connect to the AWS access portal. The link will be valid for up to 7 days. You can grant this user permissions to accounts or applications so that they can access their assigned AWS accounts and cloud applications when they sign in to the AWS access portal." Below this message is a table of users. The table has a header row with columns: "Username", "Display name", "Status", "MFA devices", and "Created by". There are nine rows of data, each representing a user: Jasmine-TKH (Jasmine Melton, Enabled, None, Manual), Edgardo-TKH (Edgardo Vasquez, Enabled, 1 device, Manual), Awa-TKH (Awa Afo, Enabled, 1 device, Manual), Takala-TKH (Takala Crook, Enabled, 1 device, Manual), Jesus-TKH (Jesus Ayala, Enabled, None, Manual), Giovanni-TKH (Giovanni Garcia, Enabled, 1 device, Manual), Jaelin-TKH (Jaelin Lazenberry, Enabled, 1 device, Manual), and Raven-TKH (raven nem, Enabled, None, Manual). The top of the screen shows the URL "us-east-1.console.aws.amazon.com/singlesignon/home?region=us-east-1#/instances/72237cee10da5dde/users\$addUserWizard" and the AWS logo.

Username	Display name	Status	MFA devices	Created by
Jasmine-TKH	Jasmine Melton	Enabled	None	Manual
Edgardo-TKH	Edgardo Vasquez	Enabled	1 device	Manual
Awa-TKH	Awa Afo	Enabled	1 device	Manual
Takala-TKH	Takala Crook	Enabled	1 device	Manual
Jesus-TKH	Jesus Ayala	Enabled	None	Manual
Giovanni-TKH	Giovanni Garcia	Enabled	1 device	Manual
Jaelin-TKH	Jaelin Lazenberry	Enabled	1 device	Manual
Raven-TKH	raven nem	Enabled	None	Manual

- We will now set permissions for users and user group TKH-Team3

11. Go to > dashboard > permissions

The screenshot shows the IAM Identity Center Dashboard. On the left sidebar, under 'Multi-account permissions', 'AWS accounts' is selected. The main content area has a 'Central management' section with a shield icon and a note about account instances. Below it is a note about service control policies (SCPs). To the right is a 'Settings summary' panel showing instance name (TKH-team3), identity source, identity center directory, region (US East (N. Virginia)), and organization ID.

12. > Create permission sets

The screenshot shows the IAM Identity Center Permission sets page. Under 'Multi-account permissions', 'Permission sets' is selected. The main content area displays a message about customer-managed policies and boundaries. Below is a table of permission sets, showing two entries: 'PowerUserAccess' and 'AdministratorAccess'. Both entries provide full access to AWS accounts.

Permission set	Description	ARN
PowerUserAccess	Provides f...	arn:aws:sso::permissionSet/ssoins-72237cee10da5d
AdministratorAccess	Provides f...	arn:aws:sso::permissionSet/ssoins-72237cee10da5d

- You have the option of using predefined or custom permissions. Predefined permissions are pre-configured sets of permissions that define the actions a user, group, or role can perform within AWS services. Custom permissions typically refer to the ability to define and configure fine-grained permissions tailored to specific requirements beyond what is offered by predefined managed policies. In this case, we are going to add some predefined permissions.

13. Add the permissions that best fit your organization

← → 🔍 us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/instances/72237cee10da5dde/organization/permission-sets/create G 🌐 ☆ J : Other Bookmarks

aws | Services | Search [Option+S] Global ▾ Jae.I ▾

☰ Select an AWS managed policy

AdministratorAccess
Provides full access to AWS services and resources.

Billing
Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DatabaseAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

DataScientist
Grants permissions to AWS data analytics services.

NetworkAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

PowerUserAccess
Provides full access to AWS services and resources, but does not allow management of Users and groups.

ReadOnlyAccess
Provides read-only access to AWS services and resources.

SecurityAudit
The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SupportUser

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

14. Enter permission description if needed > Next

The screenshot shows the 'Specify permission set details' step of the IAM permission set creation wizard. The 'Permission set name' field contains 'ViewOnlyAccess'. The 'Description - optional' field contains 'This policy grants permissions to view resources and basic metadata across all AWS services'. The 'Session duration' dropdown is set to '1 hour'. The 'Relay state - optional' section is collapsed.

15. Review details > Create

The screenshot shows the 'Review and create' step of the IAM permission set creation wizard. It displays the 'Step 1: Select permission set type' and 'Step 2: Define permission set details' sections. In Step 1, the 'Type' is 'Predefined permission set' and the name is 'ViewOnlyAccess'. In Step 2, the 'Permission set name' is 'ViewOnlyAccess', 'Session duration' is '1 hour', and 'Description' is 'This policy grants permissions to view resources and basic metadata across all AWS services'.

16. Permission successfully created.

The screenshot shows the IAM Identity Center console with a success message: "The permission set "ViewOnlyAccess" was successfully created." Below this, there is a note about customer-managed policies and permission boundaries. A table lists the "Permission sets (8)" with one entry: "ViewOnlyAccess".

Permission set	Description	ARN
ViewOnlyAccess	This policy ...	arn:aws:sso:::permissionSet/ssoins-72237cee10da5dde:ViewOnlyAccess

- Continue to repeat this process until all the permissions you wish to have are added.
- We are now going to assign permissions to certain users.

17. Click the “AWS accounts” tab > management access account

The screenshot shows the AWS accounts section of the IAM Identity Center. It displays the organizational structure with a root account named "Jae.I" which is a "management account". Account details include the ARN and email address.

Account	ARN	Email
Jae.I	891377068956	jlazenberry.fellow@theknowledgehouse.org

Permissions assigned to this account are listed as "AdministratorAccess | Billing | NetworkAdministrator | 4 more".

18. >assign users or groups

Overview

Account name Jae.l	Account ID 891377068956	Email jlazberry.fellow@theknowledgehouse.org
-----------------------	----------------------------	---

Users and groups (5) | **Permission sets (7)**

Assigned users and groups (5)

Change permission sets | Remove access | **Assign users or groups** |

The following users and groups in IAM Identity Center can select this AWS account from within their AWS access portal. [Learn more](#)

Find users by username, find groups by group name

Username / group name	Permission sets	Type
NetworkAdministrator		

- To assign permissions to a user, pick “user” tab. To assign permissions to a group, pick “group” tab. In this case i’ll pick a user.

Step 1
Select users and groups

Step 2
Select permission sets

Step 3
Review and submit

Assign users and groups to "Jae.l"

Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.

Users (7)

Users | **Create users**

<input type="checkbox"/> Username	Display name	Status
<input type="checkbox"/> Jesus-TKH	Jesus Ayala	Enabled
<input type="checkbox"/> Jaelin-TKH	Jaelin Lazenberry	Enabled
<input type="checkbox"/> Edgardo-TKH	Edgardo Vasquez	Enabled
<input type="checkbox"/> Awa-TKH	Awa Afo	Enabled

19. Go to the user you wish to assign permissions to > Next

The screenshot shows the AWS IAM Identity Center console. At the top, there's a search bar and a navigation bar with tabs like 'Services' and 'Global'. Below the search bar is a table header with columns: 'Username', 'Display name', and 'Status'. The table lists several users: Awa-Afo (selected), Jaelin-TKH, Giovanni-TKH, Takala-TKH, Jesus-TKH, Edgardo-TKH, and Jasmine-TKH. All users are marked as 'Enabled'. Below the table is a section titled 'Selected users and groups (1)'. At the bottom right of the page are buttons for 'Cancel' and 'Next'.

20. Pick the permissions you want to assign > Next > Submit

The screenshot shows the 'Review and submit' step of the IAM Identity Center configuration. It displays a table of 'Permission sets (8)'. The table has columns: 'Permission set', 'Description', and 'ARN'. Three permission sets are listed: 'ViewOnlyAccess', 'PowerUserAccess', and 'AdministratorAccess'. The 'ViewOnlyAccess' row has a checked checkbox next to it. The 'PowerUserAccess' and 'AdministratorAccess' rows have unchecked checkboxes. At the bottom right of the page are buttons for 'Cancel', 'Next', and 'Submit'.

21. Permissions successfully assigned

The screenshot shows the AWS IAM Identity Center console. The URL in the address bar is `us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/instances/72237cee10da5dde/organization/accounts/details/89137706895...`. The top navigation bar includes links for AWS Services, a search bar, and account information for `Jae.l`. A green banner at the top right states: "We reprovisioned your AWS account successfully and applied the updated permission set to the account." The left sidebar has a tree view with nodes like "Managing instance", "Dashboard", "Users", "Groups", "Settings", "Multi-account permissions" (with "AWS accounts" expanded), and "Application assignments" (with "Applications" expanded). The main content area is titled "Jae.l" and shows an "Overview" section with account details: Account name `Jae.l`, Account ID `891377068956`, and Email `jlazenberry.fellow@theknowledgehouse.org`. Below this are tabs for "Users and groups (6)" and "Permission sets (7)". The "Users and groups" tab is selected, showing a list of assigned users and groups. At the bottom of the page are links for CloudShell, Feedback, and various legal notices.

- We have successfully added permissions to a user, you can repeat this same process to add permissions to a group.