



Ajoutez des utilisateurs à votre organisation Console

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

- Ajoutez des utilisateurs à votre organisation Console 1
 - Ajouter des utilisateurs à une organisation NetApp Console 1
 - Comprendre comment l'accès est accordé dans la NetApp Console 1
 - Ajoutez des membres à votre organisation 1
 - Ajoutez un groupe fédéré à votre organisation 3
 - Informations connexes 4

Ajoutez des utilisateurs à votre organisation Console

Ajouter des utilisateurs à une organisation NetApp Console

Dans la console, vous accordez aux utilisateurs l'accès aux projets ou aux dossiers en fonction d'un rôle d'accès. Un *rôle d'accès* contient un ensemble d'autorisations qui permet à un membre (compte utilisateur ou compte de service) d'effectuer des actions spécifiques au niveau assigné de la hiérarchie des ressources.

Rôles d'accès requis

Super administrateur, administrateur d'organisation ou administrateur de dossier ou de projet (pour les dossiers et les projets qu'ils administrent). ["En savoir plus sur les rôles d'accès"](#).

Comprendre comment l'accès est accordé dans la NetApp Console

La NetApp Console utilise le contrôle d'accès basé sur les rôles (RBAC) pour gérer les autorisations. Attribuer des rôles aux utilisateurs individuellement ou par le biais de groupes fédérés. Chaque rôle définit les actions autorisées pour des ressources spécifiques.

Veillez noter les points suivants concernant l'octroi d'accès dans la NetApp Console:

- Tous les utilisateurs doivent d'abord s'inscrire à la NetApp Console avant de pouvoir accéder aux ressources.
- Vous devez attribuer explicitement un rôle à chaque utilisateur dans la console avant qu'il puisse accéder aux ressources, même s'il est membre d'un groupe fédéré auquel un rôle a été attribué.
- Vous pouvez ajouter des comptes de service directement depuis la console et leur attribuer des rôles.

Ajoutez des membres à votre organisation

La NetApp Console prend en charge trois types de membres : les comptes d'utilisateurs, les comptes de service et les groupes fédérés.

Les utilisateurs doivent s'inscrire à la NetApp Console avant que vous puissiez les ajouter et leur attribuer un rôle, même s'ils font partie d'un groupe fédéré. Créez des comptes de service directement dans la console.

Pour accéder aux ressources, tous les membres doivent se voir attribuer au moins un rôle explicite.

Lors de l'ajout d'un membre, choisissez le niveau de ressource (organisation, dossier ou projet) et attribuez-lui un ou plusieurs rôles avec les autorisations nécessaires.

Ajouter un utilisateur

Les utilisateurs s'inscrivent à la NetApp Console, mais un administrateur d'organisation, de dossier ou de projet doit les ajouter à une organisation, un dossier ou un projet pour qu'ils puissent accéder aux ressources.

Avant de commencer :

L'utilisateur doit déjà s'être inscrit à la NetApp Console. S'ils ne se sont pas encore inscrits, dirigez-les vers ["Inscrivez-vous à la NetApp Console."](#)



Si vous ajoutez un utilisateur faisant partie d'un groupe fédéré, assurez-vous que cet utilisateur s'est déjà inscrit à la NetApp Console et qu'un rôle lui a été explicitement attribué dans la console. NetApp recommande d'attribuer un rôle d'accès minimal tel que celui de lecteur de l'organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.
4. Pour **Type de membre**, gardez **Utilisateur** sélectionné.
5. Pour **E-mail de l'utilisateur**, saisissez l'adresse e-mail de l'utilisateur associée à la connexion qu'il a créée.
6. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

Notez ce qui suit :

- Vous pouvez sélectionner uniquement les dossiers et les projets pour lesquels vous disposez des autorisations.
 - Lorsque vous sélectionnez une organisation ou un dossier, vous accordez au membre l'autorisation d'accéder à tout son contenu.
 - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
7. **Sélectionnez une catégorie** puis sélectionnez un **Rôle** qui fournit au membre des autorisations pour les ressources associées à l'organisation, au dossier ou au projet que vous avez sélectionné.

["En savoir plus sur les rôles d'accès"](#) .

8. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.
9. Sélectionnez **Ajouter**.

La console envoie des instructions par courriel à l'utilisateur.

Ajouter un compte de service

Les comptes de service vous permettent d'automatiser les tâches et de vous connecter en toute sécurité aux API de la console. Choisissez un ID client et un secret pour les configurations simples, ou un JWT (JSON Web Token) pour une sécurité renforcée dans les environnements automatisés ou natifs du cloud. Choisissez la méthode qui répond à vos exigences de sécurité.

Avant de commencer :

Pour l'authentification JWT, préparez votre clé publique ou votre certificat.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.

4. Pour **Type de membre**, sélectionnez **Compte de service**.
5. Saisissez un nom pour le compte de service.
6. Pour utiliser l'authentification JWT, sélectionnez **Utiliser l'authentification JWT par clé privée** et téléchargez votre clé ou certificat RSA public. Ignorez cette étape si vous utilisez un ID client et un secret.

Votre certificat X.509. Il doit être au format PEM, CRT ou CER.

- a. Configurez les notifications d'expiration de votre certificat. Choisissez entre sept jours ou 30 jours. Les notifications d'expiration sont envoyées par e-mail et affichées dans la console aux utilisateurs ayant le rôle de super administrateur ou d'administrateur d'organisation.
7. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

Notez ce qui suit :

- Vous ne pouvez sélectionner que les dossiers et les projets pour lesquels vous disposez d'autorisations.
 - La sélection d'une organisation ou d'un dossier accorde au membre des autorisations sur tout son contenu.
 - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
8. Sélectionnez une **Catégorie**, puis un **Rôle** qui confère au membre les autorisations nécessaires pour accéder aux ressources de l'organisation, du dossier ou du projet que vous avez sélectionné.

["En savoir plus sur les rôles d'accès"](#) .

9. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.
10. Si vous n'avez pas choisi d'utiliser l'authentification JWT, téléchargez ou copiez l'ID client et le secret client.

La console n'affiche le secret client qu'une seule fois. Copiez-le en lieu sûr ; vous pourrez le recréer plus tard si vous le perdez.

11. Si vous avez choisi l'authentification JWT, téléchargez ou copiez l'ID client et l'audience JWT. La console n'affiche ces informations qu'une seule fois et ne permet pas de les récupérer ultérieurement.
12. Sélectionnez **Fermer**.

Ajoutez un groupe fédéré à votre organisation

Vous pouvez ajouter un groupe fédéré de votre fournisseur d'identité (IdP) à votre organisation et lui attribuer un ou plusieurs rôles. Les membres du groupe fédéré héritent des rôles que vous attribuez au groupe dans la console.

Avant d'attribuer un rôle à un groupe fédéré, assurez-vous des points suivants :

- Configurez la fédération entre votre fournisseur d'identité et la console. ["Apprenez à configurer une fédération."](#)
- Le groupe doit déjà exister dans votre fournisseur d'identité et avoir un accès applicatif à la console.
- Les utilisateurs appartenant au groupe doivent déjà s'être inscrits à la NetApp Console et s'être vu attribuer explicitement un rôle dans la console. NetApp recommande d'attribuer un rôle d'accès minimal tel que

celui de lecteur de l'organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.
4. Pour **Type de membre**, sélectionnez **Groupe fédéré**.
5. Sélectionnez la fédération dont le groupe est membre.
6. Pour **Nom du groupe**, veuillez saisir le nom exact du groupe dans votre fournisseur d'identité.
7. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

Notez ce qui suit :

- Vous ne pouvez sélectionner que les dossiers et les projets pour lesquels vous disposez d'autorisations.
 - La sélection d'une organisation ou d'un dossier accorde au membre des autorisations sur tout son contenu.
 - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
8. Sélectionnez une **Catégorie**, puis un **Rôle** qui confère au membre les autorisations nécessaires pour accéder aux ressources de l'organisation, du dossier ou du projet que vous avez sélectionné.

["En savoir plus sur les rôles d'accès"](#) .

9. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.

Informations connexes

- ["En savoir plus sur la gestion des identités et des accès dans la NetApp Console"](#)
- ["Démarrer avec l'identité et l'accès"](#)
- ["Rôles d'accès à la NetApp Console"](#)
- ["En savoir plus sur l'API pour l'identité et l'accès"](#)

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.