Gérer l'accès des utilisateurs et la sécurité

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

Gérer l’accès des utilisateurs et la sécurité . . . 1
- Découvrez le contrôle d’accès basé sur les rôles (RBAC) de NetApp Console . . . 1
  - Types de membres de l’organisation Console . . . 1
  - Rôles prédéfinis dans la NetApp Console . . . 1
- Gérer l’accès des membres dans la NetApp Console . . . 2
  - Comprendre comment l’accès est accordé dans la NetApp Console . . . 2
  - Afficher les membres de l’organisation . . . 3
  - Afficher les rôles attribués à un membre . . . 3
  - Afficher les membres associés à un dossier ou à un projet . . . 3
  - Attribuer ou modifier l’accès des membres . . . 4
  - Ajouter un rôle d’accès à un membre . . . 4
  - Modifier le rôle attribué à un membre . . . 5
  - Supprimer un membre de votre organisation . . . 5
- Sécurité des utilisateurs . . . 6
  - Réinitialiser les mots de passe des utilisateurs (utilisateurs locaux uniquement) . . . 6
  - Gérer l’authentification multifacteur (MFA) d’un utilisateur . . . 6
  - Recréer les informations d’identification pour un compte de service . . . 7

Gérer l’accès des utilisateurs et la sécurité

Découvrez le contrôle d’accès basé sur les rôles (RBAC) de NetApp Console

Gérez l’accès des utilisateurs à la NetApp Console grâce au contrôle d’accès basé sur les rôles (RBAC), en attribuant des rôles prédéfinis au niveau de l’organisation, du dossier ou du projet. Chaque rôle octroie des autorisations spécifiques qui définissent les actions que les utilisateurs peuvent effectuer dans le cadre de leur rôle.

NetApp conçoit les rôles de console selon le principe du moindre privilège, de sorte que chaque rôle n’inclut que les autorisations nécessaires à ses tâches. Cette approche renforce la sécurité en limitant l’accès à ce dont chaque membre a besoin.

Après avoir organisé les ressources en dossiers et projets, attribuez aux membres de l’organisation un ou plusieurs rôles pour des dossiers ou projets spécifiques, leur permettant ainsi d’exercer uniquement leurs responsabilités.

Par exemple, vous pouvez attribuer à un membre le rôle d’administrateur de résilience aux ransomwares pour un niveau de projet spécifique, lui permettant d’effectuer des opérations de résilience aux ransomwares pour les ressources de ce projet, sans lui accorder un accès plus large à l’ensemble de l’organisation. Ce même utilisateur peut se voir attribuer ce rôle pour plusieurs projets au sein de votre organisation.

Vous pouvez attribuer aux utilisateurs plusieurs rôles pour un même périmètre ou pour des périmètres différents, en fonction de leurs responsabilités. Par exemple, une petite organisation pourrait confier la gestion de la résilience aux ransomwares et des tâches de sauvegarde et de restauration à un même utilisateur au niveau de l’organisation, tandis qu’une plus grande organisation pourrait affecter des utilisateurs différents à chaque rôle au niveau du projet.

Types de membres de l’organisation Console

Il existe trois types de membres dans une organisation NetApp Console : * *Comptes utilisateurs* : Utilisateurs individuels qui se connectent à la NetApp Console pour gérer les ressources. Les utilisateurs doivent s’inscrire à la NetApp Console avant de pouvoir être ajoutés à une organisation. * *Comptes de service* : Comptes non humains utilisés par les applications ou les services pour interagir avec la NetApp Console via des API. Vous pouvez ajouter des comptes de service directement à votre organisation Console. * *Groupes fédérés* : Groupes synchronisés depuis votre fournisseur d’identité (IdP) qui vous permettent de gérer collectivement l’accès de plusieurs utilisateurs. Chaque utilisateur d’un groupe fédéré doit s’être inscrit à la NetApp Console et avoir été ajouté à votre organisation avec un rôle d’accès avant de pouvoir accéder aux ressources accordées au groupe.

"Découvrez comment ajouter des membres à votre organisation."

Rôles prédéfinis dans la NetApp Console

La NetApp Console inclut des rôles prédéfinis que vous pouvez attribuer aux membres de l’organisation. Chaque rôle comprend des autorisations qui spécifient les actions qu’un membre peut effectuer dans le cadre qui lui est assigné (organisation, dossier ou projet).

Les rôles de la NetApp Console utilisent le principe du moindre privilège, qui garantit que les membres ne disposent que des autorisations nécessaires à leurs tâches, et catégorisent les rôles selon le type d’accès

qu’ils fournissent :

- Rôles de la plateforme : Fournir les autorisations d’administration de la console
- Rôles des services de données : octroient des autorisations pour la gestion de services de données spécifiques, tels que la résilience aux ransomwares et la sauvegarde et la restauration.
- Rôles de l’application : Fournir les autorisations de gestion du stockage ainsi que d’audit des événements et alertes de la console.

Vous pouvez attribuer plusieurs rôles à un membre en fonction de ses responsabilités. Par exemple, vous pouvez attribuer à un membre à la fois le rôle d’administrateur de la résilience aux ransomwares et le rôle d’administrateur de la sauvegarde et de la récupération pour un projet spécifique.

"Découvrez les rôles prédéfinis disponibles dans la NetApp Console.".

Gérer l’accès des membres dans la NetApp Console

Gérez l’accès des membres dans votre organisation Console. Attribuer des rôles pour définir les autorisations. Supprimez les membres lorsqu’ils quittent l’entreprise.

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). Lien : reference-iam-predefined-roles.html [En savoir plus sur les rôles d’accès].

Vous pouvez attribuer des rôles d’accès par projet ou par dossier. Par exemple, attribuez un rôle à un utilisateur pour deux projets spécifiques ou attribuez le rôle au niveau du dossier pour donner à un utilisateur le rôle d’administrateur de résilience aux ransomwares pour tous les projets d’un dossier.

Ajoutez vos dossiers et projets avant d’attribuer l’accès aux utilisateurs. "Apprenez à ajouter des dossiers et des projets."

Comprendre comment l’accès est accordé dans la NetApp Console

La NetApp Console utilise un modèle de contrôle d’accès basé sur les rôles (RBAC) pour gérer les autorisations des utilisateurs. Vous pouvez attribuer des rôles prédéfinis aux membres individuellement ou par le biais de groupes fédérés. Vous pouvez ajouter et attribuer des rôles aux comptes de service, ainsi qu’aux groupes fédérés. Chaque rôle définit les actions qu’un membre peut effectuer sur les ressources associées.

Veuillez 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.

Utilisation de l’héritage de rôles

Lorsque vous attribuez un rôle au niveau de l’organisation, du dossier ou du projet dans NetApp Console, ce rôle est automatiquement hérité par toutes les ressources du périmètre sélectionné. Par exemple, les rôles au niveau d’un dossier s’appliquent à tous les projets qu’il contient, tandis que les rôles au niveau d’un projet

s’appliquent à toutes les ressources de ce projet.

Afficher les membres de l’organisation

Pour comprendre quelles ressources et autorisations sont disponibles pour un membre, vous pouvez afficher les rôles attribués au membre à différents niveaux de la hiérarchie des ressources de votre organisation."Découvrez comment utiliser les rôles pour contrôler l’accès aux ressources de la console."

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.

   Le tableau **Membres** répertorie les membres de votre organisation.

3. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez••• puis sélectionnez **Afficher les détails**.

Afficher les rôles attribués à un membre

Vous pouvez vérifier les rôles qui leur sont actuellement attribués.

Si vous disposez du rôle *Administrateur de dossier ou de projet*, la page affiche tous les membres de l’organisation. Cependant, vous ne pouvez afficher et gérer les autorisations des membres que pour les dossiers et les projets pour lesquels vous disposez d’autorisations. "En savoir plus sur les actions qu’un *administrateur de dossier ou de projet* peut effectuer" .

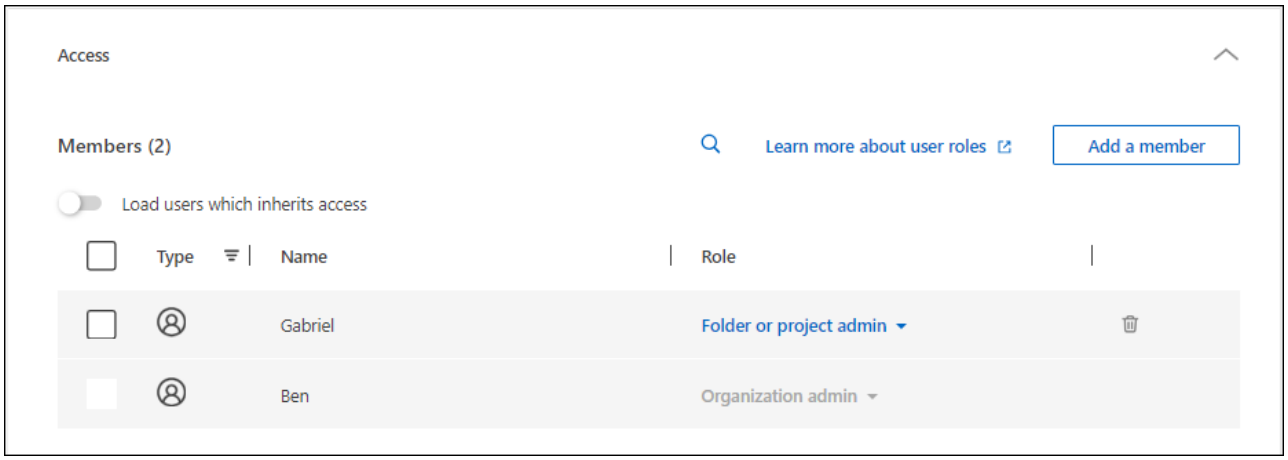
1. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
2. Dans le tableau, développez la ligne correspondante pour l’organisation, le dossier ou le projet dans lequel vous souhaitez afficher le rôle attribué au membre et sélectionnez **Afficher** dans la colonne **Rôle**.

Afficher les membres associés à un dossier ou à un projet

Vous pouvez consulter la liste des membres qui ont accès à un dossier ou à un projet spécifique.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Organisation**.
3. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
   - Sélectionnez **Accès** pour afficher les membres qui ont accès au dossier ou au projet.



Attribuer ou modifier l'accès des membres

Une fois qu'un utilisateur s'inscrit à NetApp Console, vous pouvez l'ajouter à votre organisation et lui attribuer un rôle pour lui donner accès aux ressources. "Découvrez comment ajouter des membres à votre organisation."

Vous pouvez ajuster l'accès d'un membre en ajoutant ou en supprimant des rôles selon les besoins.

Ajouter un rôle d'accès à un membre

Vous attribuez généralement un rôle lorsque vous ajoutez un membre à votre organisation, mais vous pouvez le mettre à jour à tout moment en supprimant ou en ajoutant des rôles.

Vous pouvez attribuer à un utilisateur un rôle d'accès pour votre organisation, votre dossier ou votre projet.

Les membres peuvent occuper plusieurs rôles au sein d'un même projet et dans différents projets. Par exemple, les petites organisations peuvent attribuer tous les rôles d'accès disponibles au même utilisateur, tandis que les grandes organisations peuvent confier des tâches plus spécialisées à certains utilisateurs. Vous pouvez également attribuer à un utilisateur le rôle d'administrateur de la résilience aux ransomwares au niveau de l'organisation. Dans cet exemple, l'utilisateur pourrait effectuer des tâches de résilience aux ransomwares sur tous les projets de votre organisation.

Votre stratégie de rôle d'accès doit s'aligner sur la manière dont vous avez organisé vos ressources NetApp .

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Sélectionnez le menu actions ••• à côté du membre auquel vous souhaitez attribuer un rôle et sélectionnez **Ajouter un rôle**.
5. Pour ajouter un rôle, suivez les étapes dans la boîte de dialogue :
   - **Sélectionnez une organisation, un dossier ou un projet** : Choisissez le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

     Si vous sélectionnez l'organisation ou un dossier, le membre aura des autorisations sur tout ce qui se trouve dans l'organisation ou le dossier.

- **Sélectionnez une catégorie** : Choisissez une catégorie de rôle. "En savoir plus sur les rôles d'accès" .
- Sélectionnez un **rôle** : choisissez un rôle qui fournit au membre des autorisations pour les ressources associées à l'organisation, au dossier ou au projet que vous avez sélectionné.
- **Ajouter un rôle** : si vous souhaitez fournir l'accès à des dossiers ou projets supplémentaires au sein de votre organisation, sélectionnez **Ajouter un rôle**, spécifiez un autre dossier, projet ou catégorie de rôle, puis sélectionnez une catégorie de rôle et un rôle correspondant.

6. Sélectionnez **Ajouter de nouveaux rôles**.

Modifier le rôle attribué à un membre

Modifier les rôles d'un membre pour mettre à jour son accès.

Les utilisateurs doivent avoir au moins un rôle qui leur est attribué. Vous ne pouvez pas supprimer tous les rôles d'un utilisateur. Si vous devez supprimer tous les rôles, vous devez supprimer l'utilisateur de votre organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
5. Dans le tableau, développez la ligne correspondante pour l'organisation, le dossier ou le projet pour lequel vous souhaitez modifier le rôle attribué au membre et sélectionnez **Afficher** dans la colonne **Rôle** pour afficher les rôles attribués à ce membre.
6. Vous pouvez modifier un rôle existant pour un membre ou supprimer un rôle.
   a. Pour modifier le rôle d'un membre, sélectionnez **Modifier** à côté du rôle que vous souhaitez modifier. Vous ne pouvez modifier un rôle que pour un rôle appartenant à la même catégorie de rôle. Par exemple, vous pouvez passer d'un rôle de service de données à un autre. Confirmer le changement.
   b. Pour retirer le rôle d'un membre, sélectionnez à côté du rôle pour supprimer le rôle correspondant du membre. Il vous sera demandé de confirmer la suppression.

Supprimer un membre de votre organisation

Supprimez un membre s'il quitte votre organisation.

Lorsque vous supprimez un membre, le système révoque ses autorisations de console mais conserve ses comptes de console et de site de support NetApp .

membres fédérés

- Les utilisateurs fédérés perdent automatiquement l'accès à la NetApp Console lorsqu'ils sont supprimés de votre fournisseur d'identité. Mais vous devriez tout de même les supprimer de votre organisation Console pour que votre liste de membres reste à jour.
- Si vous supprimez un utilisateur d'un groupe fédéré dans votre fournisseur d'identité, il perd l'accès à la console associé à ce groupe. Ils conservent toutefois tous les accès associés à un rôle explicite qui leur est attribué dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Supprimer l'utilisateur**.
5. Confirmez que vous souhaitez supprimer le membre de votre organisation.

Sécurité des utilisateurs

Sécurisez l'accès des utilisateurs à votre organisation NetApp Console en gérant les paramètres de sécurité des membres. Vous pouvez réinitialiser les mots de passe des utilisateurs, gérer l'authentification multifacteurs (MFA) et recréer les informations d'identification des comptes de service.

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). Lien : reference-iam-predefined-roles.html [En savoir plus sur les rôles d'accès].

Réinitialiser les mots de passe des utilisateurs (utilisateurs locaux uniquement)

Les administrateurs de l'organisation ne peuvent pas réinitialiser les mots de passe des utilisateurs locaux. Ils peuvent toutefois demander aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe.

Indiquez à l'utilisateur de réinitialiser son mot de passe depuis la page de connexion de la console en sélectionnant **Mot de passe oublié ?**.

Cette option n'est pas disponible pour les utilisateurs appartenant à une organisation fédérée.

Gérer l'authentification multifacteur (MFA) d'un utilisateur

Si un utilisateur perd l'accès à son périphérique MFA, vous pouvez supprimer ou désactiver sa configuration MFA.

L'authentification multifacteurs est uniquement disponible pour les utilisateurs locaux. Les utilisateurs fédérés ne peuvent pas activer l'authentification multifacteur.

Les utilisateurs doivent configurer à nouveau l'authentification multifacteur (MFA) lorsqu'ils se connectent après sa suppression. Si l'utilisateur perd temporairement l'accès à son dispositif MFA, il peut utiliser son code de récupération enregistré pour se connecter.

S'ils ne disposent pas de leur code de récupération, désactivez temporairement MFA pour autoriser la connexion. Lorsque vous désactivez l'authentification multifacteur pour un utilisateur, elle est désactivée pendant huit heures seulement, puis réactivée automatiquement. L'utilisateur est autorisé à se connecter une fois pendant cette période sans MFA. Après les huit heures, l'utilisateur doit utiliser MFA pour se connecter.

Pour gérer l'authentification multifacteur d'un utilisateur, vous devez disposer d'une adresse e-mail dans le même domaine que l'utilisateur concerné.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.

   Le tableau **Membres** répertorie les membres de votre organisation.

3. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Gérer l'authentification multifacteur**.
4. Choisissez de supprimer ou de désactiver la configuration MFA de l'utilisateur.

Recréer les informations d'identification pour un compte de service

Vous pouvez créer de nouveaux identifiants pour un service si vous les perdez ou si vous devez les mettre à jour.

La création de nouveaux identifiants supprime les anciens. Vous ne pouvez pas utiliser les anciens identifiants.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Dans le tableau **Membres**, accédez à un compte de service, sélectionnez ••• puis sélectionnez **Recréer les secrets**.
4. Sélectionnez **Recréer**.
5. Téléchargez ou copiez l'ID client et le secret client.

   La console n'affiche le secret client qu'une seule fois. Veillez à le copier ou à le télécharger et à le conserver en lieu sûr.

Informations sur le copyright

Informations sur les marques commerciales