ユーザーとアクセスを管理する

NetApp Console local deployment

NetApp
August 10, 2026

目次

ユーザーとアクセスを管理する

NetApp Console ローカル展開でメンバーアクセスを管理する

NetApp Console のローカル展開では、複数のフォルダーやフリートにわたるユーザーのロールを確認または変更できます。たとえば、ストレージエンジニアがアクセスできるすべての項目を確認したり、別のリージョンに新しいロールを追加したり、担当業務が変更された際にそのユーザーのアクセス権を削除したりできます。

必要なアクセスロール

スーパー管理者、組織管理者、またはフォルダ管理者もしくはフリート管理者（管理対象のフォルダおよびフリートの場合）。"アクセスロールについて"。

ニーズに応じて、アクセス権限の表示と管理を2つの方法で行うことができます。組織内のすべてのフリートにおける特定のユーザーのロールを確認したい場合は、「メンバー」ページを使用してください。

特定のフリートにアクセスできるユーザーを確認したい場合は、そのフリートに割り当てられているメンバーを確認してください。"フリートアクセス割り当ての管理"。

新しいメンバー、サービスアカウント、またはディレクトリユーザーを追加し、最初のロールを割り当てるには、代わりにオンボーディングタスクを使用してください。"メンバーを追加して役割を割り当てる"。

NetApp Console でアクセスが許可される仕組みを理解する

NetApp Console はロールベースアクセス制御（RBAC）を使用して、メンバーの権限を管理します。メンバーが必要とするアクセス範囲に応じて、組織、フォルダ、またはフリートレベルで事前定義済みのロールを割り当てることができます。

ロール継承の使用

組織レベルまたはフォルダレベルで割り当てたロールは、その下位のスコープに継承されるため、継承された割り当てを変更するには、最初に付与した上位スコープで変更する必要があります。

"NetApp Console ローカル展開におけるロール継承について".

メンバーに割り当てられた役割を表示する

変更を行う前に、メンバーがどのロールを持ち、どのスコープで権限を持っているかを正確に確認してください。例えば、チームメイトがすでに Storage admin ロールを `Production-EU-West`フリートで持っているかどうかを確認してください。

_フォルダーまたはフリート管理者_のロールを持っている場合、このページには組織内のすべてのメンバーが表示されます。ただし、アクセス権限の表示と管理は、お客様が管理するフォルダーとフリートに限られます。"NetApp Console ローカル展開におけるフォルダーまたはフリート管理者アクションについて"。

1. 「メンバー」ページから、テーブル内のメンバーに移動し、•••を選択して、「詳細を表示」を選択します。
2. 表で、メンバーに割り当てられたロールを表示する組織、フォルダー、またはフリートの該当する行を展開し、*ロール*列で*表示*を選択します。

メンバーのアクセス権の割り当てまたは変更

メンバーのアクセス権限は、担当業務が変更された際にいつでも調整できます。例えば、チームメイトが別のリージョンのバックアップ業務を担当する場合、既存のストレージロールには手を加えずに、そのリージョンのフリートにバックアップおよびリカバリの管理者ロールを追加します。

新しいメンバーを追加して最初のロールを割り当てる必要がある場合は、"メンバーを追加して役割を割り当てる"を参照してください。

既存のメンバーにアクセスロールを追加する

メンバーの責任範囲が拡大した場合は、組織、フォルダ、またはフリートレベルで、そのメンバーに追加のロールを付与してください。例えば、Storage adminに組織レベルでBackup and recovery adminロールを付与することで、既存のストレージ権限を失うことなく、すべてのフリートにわたるバックアップおよびリカバリタスクを管理できるようになります。

組織、フォルダ、またはフリートに対して、メンバーにアクセスロールを割り当てることができます。

メンバーは、同じフリート内だけでなく、異なるフリートにおいても複数のロールを担うことができます。例えば、小規模な組織では利用可能なすべてのアクセスロールを同じユーザーに割り当てる場合がある一方、大規模な組織ではユーザーに、より専門的なタスクを割り当てる場合があります。あるいは、組織レベルで特定のユーザーにランサムウェア対策管理者ロールを割り当てることもできます。この例では、ユーザーは組織内のすべてのフリートに対してランサムウェア対策タスクを実行できるようになります。

アクセスロール戦略は、NetAppリソースの整理方法と整合している必要があります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. 「メンバー」を選択します。
3. メンバータブのいずれかを選択します：「Users」、「Directory users」、または「Service accounts」。
4. 役割を割り当てるメンバーの横にあるアクションメニュー ••• を選択し、「役割を追加」を選択します。
5. 役割を追加するには、ダイアログボックスの手順を実行してください：
   - 組織、フォルダー、またはフリートを選択：メンバーに権限を付与するリソース階層のレベルを選択してください。

     組織またはフォルダを選択すると、そのメンバーは組織またはフォルダ内のすべてのコンテンツに対するアクセス権を持ちます。

   - カテゴリを選択してください：役割のカテゴリを選択してください。"アクセスロールについて"。
   - *役割*を選択：選択した組織、フォルダー、またはフリートに関連付けられたリソースに対する権限をメンバーに付与する役割を選択してください。
   - 役割の追加：組織内の追加のフォルダーまたはフリートへのアクセスを許可する場合は、*役割の追加*を選択し、別のフォルダーまたはフリートまたは役割カテゴリを指定してから、役割カテゴリと対応する役割を選択します。
6. 「新しいロールを追加」を選択します。

メンバーに割り当てられた役割を変更する

メンバーの責任範囲が変わった場合は、そのメンバーの既存のロールを別のロールに置き換えます。例えば、`Production-US-East`フリートのストレージビューアにストレージ管理者ロールが必要になった場合などです。

各ユーザーは少なくとも1つのロールを持つ必要があります。ユーザーからすべてのロールを削除することはできません。すべてのロールを削除する必要がある場合は、組織からユーザーを削除してください。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. 「メンバー」を選択します。
3. メンバータブのいずれかを選択します：「Users」、「Directory users」、または「Service accounts」。
4. 「メンバー」ページから、テーブル内のメンバーに移動し、…を選択して、「詳細を表示」を選択します。
5. 表で、メンバーに割り当てられたロールを変更する組織、フォルダー、またはフリートの該当する行を展開し、*ロール*列の*表示*を選択して、このメンバーに割り当てられているロールを確認します。
6. メンバーの既存の役割を変更したり、役割を削除したりできます。
   a. メンバーの役割を変更するには、変更したい役割の横にある「変更」を選択してください。役割を変更できるのは、同じ役割カテゴリ内の役割のみです。例えば、あるデータサービスロールから別のデータサービスロールに変更することができます。変更内容を確認してください。
   b. メンバーの役割の割り当てを解除するには、役割の横にある を選択して、メンバーから該当の役割を解除します。削除の確認を求められます。

組織からメンバーを削除する

組織を離れる場合、またはConsoleへのアクセスが不要になるような役割変更があった場合は、メンバーを削除してください。例えば、契約社員との契約が終了した場合や、従業員がConsole組織外のチームに異動した場合などが挙げられます。

ディレクトリユーザー

ディレクトリからユーザーを削除すると、そのユーザーは認証できなくなります。メンバーリストの正確性を維持し、Console のローカル展開で割り当てられたロールを削除するために、ユーザーを Console 組織から削除する必要があります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. 「メンバー」を選択します。
3. メンバータブのいずれかを選択します：「Users」、「Directory users」、または「Service accounts」。
4. 「メンバー」ページから、テーブル内のメンバーに移動し、…を選択してから「ユーザーを削除」を選択します。
5. 組織からそのメンバーを削除することを確認してください。

NetApp Console ローカル展開でのフリートアクセス割り当ての表示または変更

フォルダーとストレージ フリートのメンバー アクセス割り当てを監査または変更するには、NetApp Console ローカル展開を使用します。フォルダ管理者やフリート管理者は、通常このビューから作業を行います。このビューには、管理対象のスコープのみが表示されるためです。

必要なアクセスロール

スーパー管理者、組織管理者、フォルダ管理者、またはフリート管理者。"アクセスロールについて"。

あるいは、特定のメンバーのすべてのロールを複数のフォルダーやフリートにわたって管理することもできます。"メンバーアクセスを管理する"。

フォルダーとフリートへのアクセス方法

コンソールのローカル展開では、ロールベースのアクセス制御（RBAC）を使用します。フォルダレベルで割り当てたロールは、そのフォルダ内のすべてのフリートとサブフォルダに適用されます。フリートレベルで割り当てたロールは、そのフリートのリソースにのみ適用されます。"NetApp Console ローカル展開におけるロール継承について"。

メンバーがフォルダーまたは組織から役割を継承した場合、フリートレベルで役割を変更することはできません。継承されたアクセス権を変更するには、上位スコープのロールを変更してください。

フォルダまたはフリートに割り当てられたメンバーを表示する

特定のフォルダやフリートを管理できるユーザーを正確に確認してください。例えば、新しい本番環境の ONTAP クラスターを `Production-US-East`フリートに関連付ける前に、フリートの「アクセス」タブを開いて、誰がアクセス権限を持っているかを確認します。

手順

1. **[Administration]** > **[Identity and access]** を選択します。
2. **Organization** を選択します。
3. 組織ページから、テーブル内のフォルダーまたはフリートに移動し、•••を選択してから、「フォルダーの編集」または「フリートの編集」を選択します。
4. アクセス を選択すると、フォルダまたはフリートへのアクセス権を持つメンバーが表示されます。

フォルダまたはフリートからメンバーのアクセス権限を変更する

既に組織に所属しているメンバーのロールを、単一のフォルダまたはフリートに限定して調整します。例えば、チームメンバーが開発フリートから本番フリートへ移動した場合、他の環境へのアクセス権限に影響を与えることなく、本番フリートにおける Storage viewer から Storage admin へと昇格させます。

新しいメンバーを追加して最初のロールを割り当てるには、代わりにオンボーディングタスクを使用してください。"メンバーを追加して役割を割り当てる"。

手順

1. 組織ページから、テーブル内のフォルダーまたはフリートに移動し、…を選択してから、「フォルダーの編集」または「フリートの編集」を選択します。
2. 「アクセス」を選択すると、アクセス権限を持つメンバーの一覧が表示されます。
3. メンバーのアクセス権限を変更する：
   - メンバーの役割を変更する：組織管理者以外の役割を持つメンバーについては、既存の役割を選択し、新しい役割を選択します。この変更はこのスコープにのみ適用され、上位スコープから継承されたロールはここには表示されません。
   - このスコープでのメンバーアクセスを削除する：このフォルダーまたはフリートで直接ロールが定義されているメンバーの場合、ロールを削除してこのスコープでのアクセスを取り消します。これは、そのメンバーを組織から除名したり、他のスコープでのロールに影響を与えたりするものではありません。

     "組織からメンバーを削除する".
4. 「適用」を選択します。

NetApp Console ローカル展開でメンバーのセキュリティを管理する

メンバーのセキュリティ設定を管理することで、NetApp Console のローカル展開組織へのユーザーアクセスを安全に保護します。ローカルユーザーに自身のパスワードの変更を指示したり、ローカルユーザーの多要素認証（MFA）を管理したり、サービスアカウントの認証情報を再作成したりできます。

必要なアクセスロール

スーパー管理者、組織管理者、フォルダ管理者、またはフリート管理者。"アクセスロールについて"。

ユーザーパスワードのリセット（ローカルユーザーのみ）

管理者はローカルユーザーのパスワードを直接リセットすることはできません。

ローカルユーザーには、Console のローカル展開ログインページから「パスワードをお忘れですか？」を選択してパスワードをリセットするように指示してください。

このオプションはディレクトリユーザーには利用できません。

ローカルユーザーの多要素認証（MFA）を管理する

ローカルユーザーがMFAデバイスへのアクセス権を失った場合、MFA設定を削除または無効にすることができます。

多要素認証はローカルユーザーのみが利用可能です。ディレクトリユーザーは、Console のローカル展開では MFA を有効にできません。

適切な行動を選択するには、以下のガイドラインを参考にしてください。

- ユーザーが一時的に MFA デバイスへのアクセス権を失った場合は、無効にする を選択してください。MFA を無効にすると、8 時間の間は MFA なしで一度サインインできますが、その後自動的に MFA が再度有効になります。
- ユーザーがMFAを完全にリセットする必要がある場合は、「削除」を選択します。MFAを削除すると、ユーザーはMFAを再度設定するまで、MFAなしでサインインできます。

ユーザーが復旧コードを保存している場合は、それを使ってサインインできます。ユーザーが復旧コードを持っていない場合は、MFAを無効にして、ユーザーがサインインしてアクセス権を回復できるようにします。

ローカルユーザーの多要素認証を管理するには、対象ユーザーと同じドメインのメールアドレスが必要です。

手順

1. **[Administration]** > **[Identity and access]** を選択します。
2. 「メンバー」を選択します。
3. メンバーページから、テーブル内のメンバーに移動し、 を選択して、「多要素認証の管理」を選択します。
4. ユーザーのMFA設定を削除するか、無効にするかを選択します。

終了後の操作

監査ログを確認して、誰がMFAアクセスを変更したか、いつ変更したか、そしてその操作が成功したかどうかを確認してください。"NetApp Console のローカル展開アクティビティを監査する方法を学ぶ"。

サービスアカウントの認証情報を再作成する

サービスアカウントのクレデンシャルを紛失した場合や更新する必要がある場合は、新しいクレデンシャルを作成できます。

新しい認証情報を作成すると、古い認証情報は削除されます。古い認証情報は使用できません。

手順

1. **[Administration]** > **[Identity and access]** を選択します。
2. 「メンバー」を選択します。
3. メンバーテーブルで、サービスアカウントに移動し、 を選択して、「シークレットの再作成」を選択します。
4. 「再作成」を選択します。
5. クライアントIDとクライアントシークレットをダウンロードまたはコピーしてください。

   コンソールのローカルデプロイメントでは、クライアントシークレットは一度だけ表示されます。必ずコピーまたはダウンロードして、安全な場所に保管してください。

著作権に関する情報

商標に関する情報