ユーザーアクセスとセキュリティを管理する

NetApp Console setup and administration

NetApp
February 11, 2026

目次

ユーザーアクセスとセキュリティを管理する

NetApp Consoleのロールベースアクセス制御（RBAC）について学ぶ

ロールベースのアクセス制御 (RBAC) を使用してNetApp Consoleへのユーザー アクセスを管理し、組織、フォルダ、またはプロジェクト レベルで事前定義されたロールを割り当てます。各ロールは、割り当てられたスコープ内でユーザーが実行できるアクションを定義する特定の権限を付与します。

NetApp は最小限の権限でコンソール ロールを設計しているため、各ロールにはそのタスクに必要な権限のみが含まれます。このアプローチでは、各メンバーが必要なものへのアクセスを制限することでセキュリティが強化されます。

リソースをフォルダーとプロジェクトに整理した後、組織のメンバーに特定のフォルダーまたはプロジェクトに対するロールを割り当て、メンバーが自分の責任のみを実行できるようにします。

たとえば、特定のプロジェクト レベルのランサムウェア レジリエンス管理者ロールをメンバーに割り当てて、組織全体へのより広範なアクセス権を付与することなく、そのプロジェクト内のリソースに対してランサムウェア レジリエンス操作を実行できるようにすることができます。同じユーザーに、組織内の複数のプロジェクトの役割を付与できます。

ユーザーの責任に応じて、同じスコープまたは異なるスコープに対して複数のロールを割り当てることができます。たとえば、小規模な組織では、同じユーザーが組織レベルでランサムウェア耐性とバックアップとリカバリの両方のタスクを管理する可能性がありますが、大規模な組織では、プロジェクト レベルで各ロールに異なるユーザーが割り当てられている可能性があります。

コンソール組織メンバーの種類

NetApp Console組織には、次の 3 種類のメンバーがあります。 * ユーザー アカウント: リソースを管理するためにNetApp Consoleにログインする個々のユーザー。ユーザーは、組織に追加される前にNetApp Consoleにサインアップする必要があります。* サービス アカウント: API 経由でNetApp Consoleと対話するためにアプリケーションまたはサービスによって使用される人間以外のアカウント。サービス アカウントをコンソール組織に直接追加できます。* フェデレーション グループ: アイデンティティ プロバイダー (IdP) から同期されたグループで、複数のユーザーのアクセスをまとめて管理できます。フェデレーション グループ内の各ユーザーは、グループに付与されたリソースにアクセスする前に、 NetApp Consoleにサインアップし、アクセス ロールを持って組織に追加されている必要があります。

"組織にメンバーを追加する方法を学びます。"

NetApp Consoleの事前定義されたロール

NetApp Consoleには、組織のメンバーに割り当てることができる定義済みのロールが含まれています。各ロールには、割り当てられた範囲 (組織、フォルダ、またはプロジェクト) 内でメンバーが実行できるアクションを指定する権限が含まれています。

NetApp Consoleのロールでは、メンバーがタスクに必要な権限のみを持つようにする最小権限の原則が採用されており、ロールは提供されるアクセスの種類によって分類されます。

- プラットフォームの役割: コンソール管理権限を付与する
- データ サービス ロール: ランサムウェア耐性やバックアップとリカバリなどの特定のデータ サービスを管理するための権限を提供します。
- アプリケーション ロール: ストレージの管理とコンソール イベントおよびアラートの監査の権限を提供します。

メンバーの責任に基づいて、複数の役割を割り当てることができます。たとえば、特定のプロジェクトに対して、メンバーにランサムウェア耐性管理者ロールとバックアップとリカバリ管理者ロールの両方を割り当てることができます。

"NetApp Consoleで利用可能な定義済みロールについて学習します"。

NetApp Consoleでメンバーアクセスを管理する

コンソール組織内のメンバー アクセスを管理します。権限を設定するためにロールを割り当てます。メンバーが退会したら削除します。

必要なアクセスロール

スーパー管理者、組織管理者、またはフォルダーまたはプロジェクトの管理者（管理しているフォルダーとプロジェクトの場合）。リンク:reference-iam-predefined-roles.html[アクセス ロールについて学ぶ]

プロジェクトまたはフォルダーごとにアクセス ロールを割り当てることができます。たとえば、特定の 2 つのプロジェクトに対してユーザーにロールを割り当てたり、フォルダー レベルでロールを割り当てて、フォルダー内のすべてのプロジェクトに対する Ransomware Resilience 管理者ロールをユーザーに付与したりすることができます。

ユーザーにアクセスを割り当てる前に、フォルダーとプロジェクトを追加します。 "フォルダーとプロジェクトを追加する方法を学びます。"

NetApp Consoleでアクセスを許可する方法を理解する

NetApp Consoleは、ロールベースのアクセス制御 (RBAC) モデルを使用してユーザー権限を管理します。事前定義されたロールをメンバーに個別に割り当てることも、フェデレーション グループを通じて割り当てることもできます。サービス アカウントやフェデレーション グループにロールを追加して割り当てることができます。各ロールは、メンバーが関連付けられたリソースで実行できるアクションを定義します。

NetApp Consoleでアクセス権を付与する場合は、次の点に注意してください。

- すべてのユーザーは、リソースへのアクセス権を付与される前に、まずNetApp Consoleにサインアップする必要があります。
- ロールが割り当てられたフェデレーション グループのメンバーであっても、ユーザーがリソースにアクセスするには、コンソールで各ユーザーにロールを明示的に割り当てる必要があります。
- コンソールから直接サービス アカウントを追加し、ロールを割り当てることができます。

ロール継承の使用

NetApp Consoleで組織、フォルダ、またはプロジェクト レベルでロールを割り当てると、そのロールは選択したスコープ内のすべてのリソースに自動的に継承されます。たとえば、フォルダ レベルのロールはその中

に含まれるすべてのプロジェクトに適用されますが、プロジェクト レベルのロールはそのプロジェクト内のすべてのリソースに適用されます。

組織メンバーを表示

メンバーが利用できるリソースと権限を理解するには、組織のリソース階層のさまざまなレベルでメンバーに割り当てられているロールを表示できます。"ロールを使用してコンソール リソースへのアクセスを制御する方法を学習します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。

3. *メンバー*ページで、テーブル内のメンバーに移動し、 次に、[詳細を表示] を選択します。

メンバーに割り当てられた役割を表示する

現在割り当てられているロールを確認できます。

フォルダーまたはプロジェクト管理者 ロールを持っている場合、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、メンバー権限を表示および管理できるのは、権限を持つフォルダーとプロジェクトのみです。"フォルダまたはプロジェクト管理者が実行できるアクションの詳細" 。

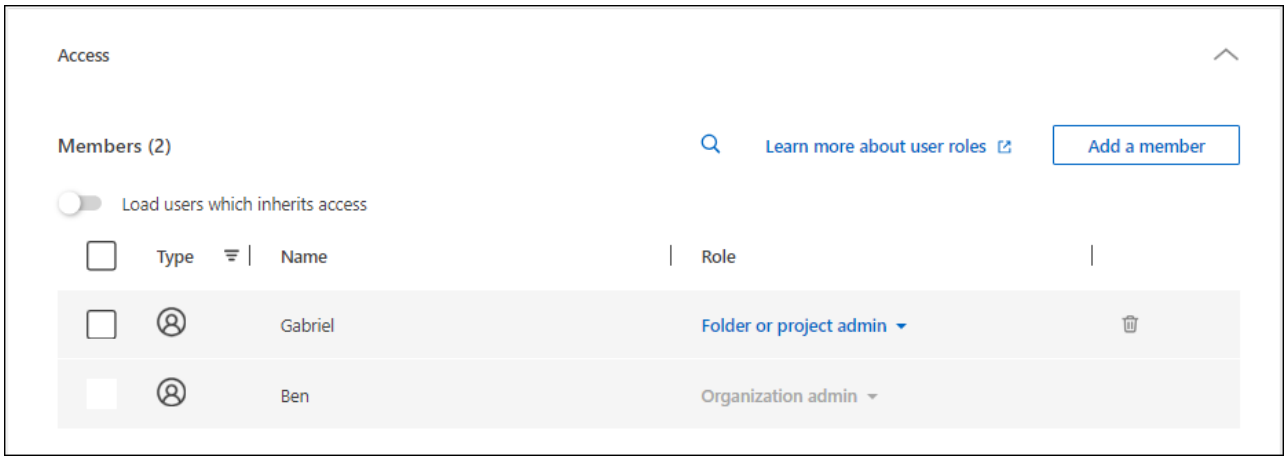
1. *メンバー*ページで、テーブル内のメンバーに移動し、 次に、[詳細を表示] を選択します。
2. 表で、メンバーに割り当てられたロールを表示する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択します。

フォルダまたはプロジェクトに関連付けられたメンバーを表示する

特定のフォルダーまたはプロジェクトにアクセスできるメンバーを表示できます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
   - フォルダーまたはプロジェクトにアクセスできるメンバーを表示するには、「アクセス」を選択します。



メンバーアクセスの割り当てまたは変更

ユーザーがNetApp Consoleにサインアップしたら、そのユーザーを組織に追加し、リソースへのアクセスを提供するロールを割り当てることができます。 "組織にメンバーを追加する方法を学びます。"

必要に応じて役割を追加または削除することで、メンバーのアクセスを調整できます。

メンバーにアクセスロールを追加する

通常、組織にメンバーを追加するときにロールを割り当てますが、ロールを削除または追加することでいつでも更新できます。

組織、フォルダ、またはプロジェクトへのアクセス ロールをユーザーに割り当てることができます。

メンバーは、同じプロジェクト内および異なるプロジェクト内で複数の役割を持つことができます。たとえば、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りますが、大規模な組織では、ユーザーにさらに専門的なタスクを実行させる場合があります。あるいは、組織レベルで 1 人のユーザーに Ransomware Resilience 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プロジェクトでランサムウェア耐性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リソースの編成方法と一致する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
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: ユーザー、サービス アカウント、または フェデレーション グループ。
4. アクションメニューを選択•••役割を割り当てるメンバーの横にある をクリックし、[役割の追加] を選択します。
5. ロールを追加するには、ダイアログ ボックスの手順を完了します。
   - 組織、フォルダ、またはプロジェクトを選択: メンバーに権限を与えるリソース階層のレベルを選択します。

     組織またはフォルダを選択した場合、メンバーにはその組織またはフォルダ内に存在するすべてのものに対する権限が付与されます。

- カテゴリを選択: 役割のカテゴリを選択します。"アクセスロールについて学ぶ" 。
- *ロール*を選択: 選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与するロールを選択します。
- ロールの追加: 組織内の追加のフォルダーまたはプロジェクトへのアクセス権を付与する場合は、*ロールの追加*を選択し、別のフォルダーまたはプロジェクトまたはロールのカテゴリを指定してから、ロールのカテゴリと対応するロールを選択します。

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

メンバーの役割を変更してアクセスを更新します。

ユーザーには少なくとも 1 つのロールが割り当てられている必要があります。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する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
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: ユーザー、サービス アカウント、または フェデレーション グループ。
4. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[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、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「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表示します。
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」を選択します。ロールを変更できるのは、同じロール カテゴリ内のロールのみです。たとえば、あるデータ サービス ロールから別のデータ サービス ロールに変更できます。変更を確認します。
   b. メンバーの役割の割り当てを解除するには、 をクリックすると、メンバーから該当するロールが削除されます。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

メンバーが組織を離れる場合は、そのメンバーを削除します。

メンバーを削除すると、そのメンバーのコンソール権限は取り消されますが、コンソールとNetApp Support Siteのアカウントは保持されます。

連合メンバー

- フェデレーション ユーザーは、IdP から削除されると、自動的にNetApp Consoleにアクセスできなくなります。ただし、メンバーリストを最新の状態に保つには、コンソール組織からそれらのメンバーを削除する必要があります。
- IdP のフェデレーション グループからユーザーを削除すると、そのグループに関連付けられているコンソール アクセスが失われます。ただし、コンソールで明示的に割り当てられたロールに関連付けられたアクセス権は引き続き保持されます。

手順

1. *管理 > IDとアクセス*を選択します。
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: ユーザー、サービス アカウント、または フェデレーション グループ。
4. メンバー*ページで、テーブル内のメンバーに移動し、 ••• 次に、[*ユーザーの削除]を選択します。
5. 組織からメンバーを削除することを確認します。

ユーザーセキュリティ

メンバーのセキュリティ設定を管理して、 NetApp Console組織へのユーザー アクセスを保護します。ユーザー パスワードをリセットしたり、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、またはフォルダーまたはプロジェクトの管理者（管理しているフォルダーとプロジェクトの場合）。リンク:reference-iam-predefined-roles.html[アクセス ロールについて学ぶ]

ユーザーパスワードをリセットする（ローカルユーザーのみ）

組織管理者はローカル ユーザーのユーザー パスワードをリセットできません。ただし、ユーザーに自分のパスワードをリセットするように指示することはできます。

コンソールのログイン ページで [パスワードを忘れた場合] を選択して、ユーザーにパスワードをリセットするよう指示します。

このオプションは、フェデレーション組織内のユーザーには使用できません。

ユーザーの多要素認証（MFA）を管理する

ユーザーが MFA デバイスにアクセスできなくなった場合は、MFA 構成を削除するか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できます。フェデレーション ユーザーは MFA を有効にできません。

ユーザーは、削除後にログインするときに、MFA を再度設定する必要があります。ユーザーが一時的に MFA

デバイスにアクセスできなくなった場合、保存した回復コードを使用してログインできます。

回復コードがない場合は、一時的に MFA を無効にしてログインを許可します。ユーザーの MFA を無効にすると、8 時間だけ無効になり、その後自動的に再度有効になります。その間、ユーザーは MFA なしで 1 回のログインが許可されます。8 時間経過後、ユーザーは MFA を使用してログインする必要があります。

ユーザーの多要素認証を管理するには、影響を受ける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. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。

3. メンバー*ページで、テーブル内のメンバーに移動し、 次に、[*多要素認証の管理]を選択します。
4. ユーザーの MFA 構成を削除するか無効にするかを選択します。

サービス アカウントの認証情報を再作成する

サービスの資格情報を紛失した場合や更新する必要がある場合は、新しい資格情報を作成できます。

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

手順

1. *管理 > IDとアクセス*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、 次に、[*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ます。

   コンソールにはクライアント シークレットが 1 回だけ表示されます。必ずコピーまたはダウンロードして安全に保管してください。