



NetApp Console ローカル展開の管理と監視

NetApp Console local deployment

NetApp
August 10, 2026

目次

NetApp Console ローカル展開の管理と監視	1
NetApp Console ローカル展開における管理と監視について学ぶ	1
監査活動	1
Licenses and subscriptions	1
コンソールのローカルデプロイメントVMの保守とトラブルシューティング	1
ユーザーとアクセスを管理する	1
NetApp Consoleのローカル デプロイ アクティビティの監査	1
監査ページからユーザーアクティビティを監査する	2
NetApp Consoleのメンテナンス	3
NetApp Consoleのローカルデプロイ用のvCenterまたはESXiホストのメンテナンス	3
ユーザーとアクセスを管理する	6
NetApp Console ローカル展開でメンバーアクセスを管理する	6
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	9
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	10

NetApp Console ローカル展開の管理と監視

NetApp Console ローカル展開における管理と監視について学ぶ

NetApp Console のローカルデプロイメントをデプロイした後、管理ツールと監視ツールを使用してアクティビティを確認し、VMを維持管理し、メンバーアクセスを管理します。

監査活動

ユーザーと API のアクティビティを確認し、NetApp Console 操作のステータスを追跡し、監査ログをダウンロードし、より長期間の保存や追加分析が必要な場合にログを外部ツールにエクスポートします。

- ["NetApp Consoleのローカル デプロイ アクティビティの監査"](#)
- ["NetApp Console ローカル展開で通知配信チャンネルを設定する"](#)

Licenses and subscriptions

ライセンスおよびサブスクリプション情報を使用して、コンソール環境におけるサービス利用資格とサブスクリプション状況を確認してください。

["ライセンスとサブスクリプションについて"](#).

コンソールのローカルデプロイメントVMの保守とトラブルシューティング

コンソールのローカル展開をホストする仮想マシン（VM）を維持管理し、ネットワークおよびシステム設定を確認し、診断ツールにアクセスし、サービスまたはエージェントが期待どおりに動作しない場合に問題のトラブルシューティングを行います。

["コンソールのローカル展開用のvCenterまたはESXiホストを管理する"](#).

ユーザーとアクセスを管理する

組織全体のメンバーアクセス権限を確認し、フリートレベルでアクセス権限を調整し、MFA復旧やサービスアカウント認証情報などのセキュリティ設定を管理します。

- ["NetApp Console でメンバーアクセスを管理する"](#)
- ["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"](#)
- ["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"](#)

NetApp Consoleのローカル デプロイ アクティビティの監査

監査ページから UI と API の両方から開始されたユーザーアクティビティを監査でき、NetApp Console のローカル展開における操作のステータスとそれを開始したユーザーを監視できます。

必須の役割

スーパー管理者、組織管理者、フォルダおよびフリート管理者、運用サポートアナリスト、スーパービューアー、組織ビューアー、またはフォルダおよびフリートビューアー。["アクセスロールについて"](#)。

コンソールのローカル展開で監査アクティビティを表示したり、監査ログのCSVをダウンロードしたり、Webhookを使用して監査ログをお客様独自のsyslogサーバーに送信するように設定したりできます。

監査ページからユーザーアクティビティを監査する

監査ページを使用して、誰がどのような操作を行ったか、またはその操作のステータスを確認できます。

監査ページには、組織内でユーザーが行った操作が表示されます。例えば、誰が組織にメンバーを追加したか、フリートが正常に削除されたかを確認できるほか、組織内でユーザーが行ったその他のストレージ管理操作も確認できます。

監査ログには、以下のサービスのアクティビティが表示されます：

- テナント管理：ユーザーの追加、フリートの作成、リソースの関連付けなど、組織の管理に関連する操作。
- ストレージ管理：ストレージリソースの管理に関連する操作。
- フェデレーション：フェデレーションの管理に関連する操作。例えば、フェデレーションの作成、フェデレーション組織の追加または削除など。

手順

1. *「管理」>「監査」*を選択してください。
2. 表の上にあるフィルターを使用して、表に表示されるアクションを変更できます。

例えば、サービス フィルターを使用して特定のサービスに関連するアクションを表示したり、ユーザー フィルターを使用して特定のユーザーアカウントに関連するアクションを表示したりできます。

IDとアクセス管理アクションの監査ログをフィルタリングする

メンバーの追加、フリートの作成、リソースの削除など、組織の管理に関連する操作のみを表示するには、監査ログをTenancyサービスでフィルタリングします。

手順

1. *「管理」>「監査」*を選択してください。
2. フィルターを使用して結果を絞り込んでください。「サービス」を選択し、次に「テナント」を選択してください。
3. 結果をさらに絞り込むには、他のフィルターを使用してください。

例えば、*ユーザー*フィルターを使用して、特定のユーザーアカウントによって実行されたIAMアクションを表示します。

監査ページから監査ログをダウンロードする

監査ページから監査ログをCSVファイルとしてダウンロードできます。これにより、組織内でユーザーが行った操作の記録を保持することができます。ダウンロードされたCSVファイルには、監査ページのフィルターや

表示列に関係なく、すべての監査ログ列が含まれます。

手順

1. 「監査」 ページで、表の右上隅にあるダウンロードアイコンを選択します。

NetApp Consoleのメンテナンス

NetApp Consoleのローカルデプロイ用のvCenterまたはESXiホストのメンテナンス

NetApp Console ローカルデプロイメントでは、コンソールローカルデプロイメントをデプロイした後でも、既存の vCenter または ESXi ホストに変更を加えることができます。たとえば、コンソールローカルデプロイメントをホストする VM インスタンスの CPU や RAM を増やすことができます。

VMウェブコンソールを使用して、以下のメンテナンス作業を実行します。

- ディスクサイズを増やす
- コンソールのローカル展開を再起動します
- 静的ルートを更新する
- 検索ドメインを更新する

制限事項

メンテナンスコンソールでは、IPアドレス、DNS、ゲートウェイに関する情報を閲覧することのみ可能で、更新はできません。

VMメンテナンスコンソールにアクセスします

vSphereクライアントからメンテナンスコンソールにアクセスできます。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。

maintユーザーのパスワードを変更する

`maint`ユーザーのパスワードを変更できます。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。

3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. 入力 `1` して `System Configuration` メニューを表示します。
6. `1` を入力してメンテナンスユーザーのパスワードを変更し、画面の指示に従ってください。

VMインスタンスのCPUまたはRAMを増やす

コンソールのローカル展開をホストする VM インスタンスの CPU または RAM を増やすことができます。

VCenter または ESXi ホストで VM インスタンスの設定を編集し、メンテナンスコンソールを使用して変更を適用します。

vSphereクライアントでの手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. VMインスタンスを右クリックして、*設定の編集*を選択します。
4. /opt または /var パーティションに使用されているハードドライブの容量を増やしてください。
 - a. /opt に使用されるハードドライブの容量を増やすには、「ハードディスク 2」を選択します。
 - b. /var に使用されるハードドライブの容量を増やすには、「ハードディスク 3」を選択します。
5. 変更を保存します。

メンテナンスコンソールでの手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. 入力 `1 to view the` `System Configuration` メニュー。
6. 入力 `2` して、画面の指示に従ってください。コンソールは新しい設定をスキャンし、パーティションのサイズを拡大します。

コンソールのローカル展開VMのネットワーク設定を表示する

ネットワークの問題を確認またはトラブルシューティングするには、vSphereクライアントでコンソールローカルデプロイメントVMのネットワーク設定を表示します。以下のネットワーク設定は表示のみ可能で、更新はできません：IPアドレスとDNSの詳細。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。

4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. `2` を入力して `Network Configuration` メニューを表示します。
6. 1から6までの数字を入力すると、対応するネットワーク設定が表示されます。

コンソールローカルデプロイメント**VM**の静的ルートを更新します

必要に応じて、コンソールローカルデプロイメントVMの静的ルートを追加、更新、または削除します。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. `2` を入力して `Network Configuration` メニューを表示します。
6. 静的ルートを更新するには、`7` を入力し、画面の指示に従ってください。
7. Enterキーを押します。
8. 必要に応じて、さらに変更を加えてください。
9. `9` を押して変更を確定します。

コンソールローカル展開**VM**のドメイン検索設定を更新する

コンソールのローカルデプロイメントVMの検索ドメイン設定を更新できます。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. `2` を入力して `Network Configuration` メニューを表示します。
6. 入力 `8` してドメイン検索設定を更新し、画面の指示に従ってください。
7. Enterキーを押します。
8. 必要に応じて、さらに変更を加えてください。
9. `9` を押して変更を確定します。

コンソールのローカル展開診断ツールにアクセスする

コンソールのローカル展開に関する問題をトラブルシューティングするには、診断ツールにアクセスしてください。NetApp サポートから、問題のトラブルシューティング時にこの操作を求められる場合があります。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. `3` を入力して、サポートと診断メニューを表示します。
6. 入力 `1` して診断ツールにアクセスし、画面の指示に従ってください。

コンソールのローカル展開診断ツールにリモートでアクセスする

Puttyなどのツールを使用して、診断ツールにリモートでアクセスできます。ワンタイムパスワードを割り当てることで、コンソールのローカルデプロイメントVMへのSSHアクセスを有効にします。

SSHアクセスにより、コピー＆ペーストなどの高度なターミナル機能を利用できるようになります。

手順

1. vSphereクライアントを開き、vCenterにログインしてください。
2. Console のローカル展開をホストする VM インスタンスを選択します。
3. 「Launch Web Console」を選択します。
4. VMインスタンス作成時に指定したユーザー名とパスワードを使用して、VMインスタンスにログインします。ユーザー名は `maint` で、パスワードはVMインスタンス作成時に指定したものです。
5. `3` を入力して `Support and Diagnostics` メニューを表示します。
6. `2` を入力して診断ツールにアクセスし、画面の指示に従って24時間で有効期限が切れるワンタイムパスワードを設定してください。
7. PuttyなどのSSHツールを使用して、ユーザー名 `diag` と設定したワンタイムパスワードを使用して、コンソールのローカルデプロイメントVMに接続します。

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

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またはフリートに移動し、**...**を選択してから、「フォルダの編集」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またはフリートに移動し、**...**を選択してから、「フォルダの編集」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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。