NetApp Consoleを使用する

NetApp Console setup and administration

NetApp
January 23, 2026

目次

NetApp Consoleを使用する

NetApp Consoleにログインする

NetApp Consoleにログインする方法は、使用している展開モードによって異なります。

24 時間経過またはブラウザを閉じると、自動的にログアウトされます。

"コンソールの展開モードについて学ぶ" 。

標準モード

NetApp Consoleにサインアップすると、Web ベースのコンソールからログインして、データとストレージ インフラストラクチャの管理を開始できます。

タスク概要

次のいずれかのオプションを使用してNetApp Consoleにログインできます。

- 既存のNetAppサポートサイト（NSS）の認証情報
- メールアドレスとパスワードを使用したNetApp Consoleアカウント
- フェデレーション接続

  シングル サインオンを使用すると、企業ディレクトリ (フェデレーション ID) の資格情報を使用してログインできます。"ID連携の設定方法を学ぶ" 。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. *ログイン*ページで、ログインに関連付けられているメールアドレスを入力します。
3. ログインに関連付けられた認証方法に応じて、資格情報を入力するよう求められます。
   - NetAppクラウド認証情報: パスワードを入力してください
   - フェデレーションユーザー: フェデレーションIDの資格情報を入力してください
   - NetAppサポートサイトアカウント: NetAppサポートサイトの認証情報を入力します

結果

これでログインが完了し、ハイブリッド マルチクラウド インフラストラクチャの管理を開始できるようになりました。

制限モード

コンソールを制限モードで使用する場合は、エージェント上でローカルに実行されるユーザー インターフェイスからコンソールにログインする必要があります。

タスク概要

コンソールは、制限モードの場合、次のいずれかのオプションを使用してログインすることをサポートします。

- メールアドレスとパスワードを使用したNetApp Consoleログイン
- フェデレーション接続

  シングル サインオンを使用すると、企業ディレクトリ (フェデレーション ID) の資格情報を使用してログインできます。"アイデンティティフェデレーションの使い方を学ぶ" 。

手順

1. Web ブラウザを開き、エージェントがインストールされている IP アドレスを入力します。
2. ユーザー名とパスワードを入力してログインしてください。

複数のコンソールエージェントを操作する

複数のコンソール エージェントを使用する場合は、コンソールから直接それらのコンソール エージェントを切り替えて、関連付けられているシステムを表示できます。

コンソールエージェントを切り替える

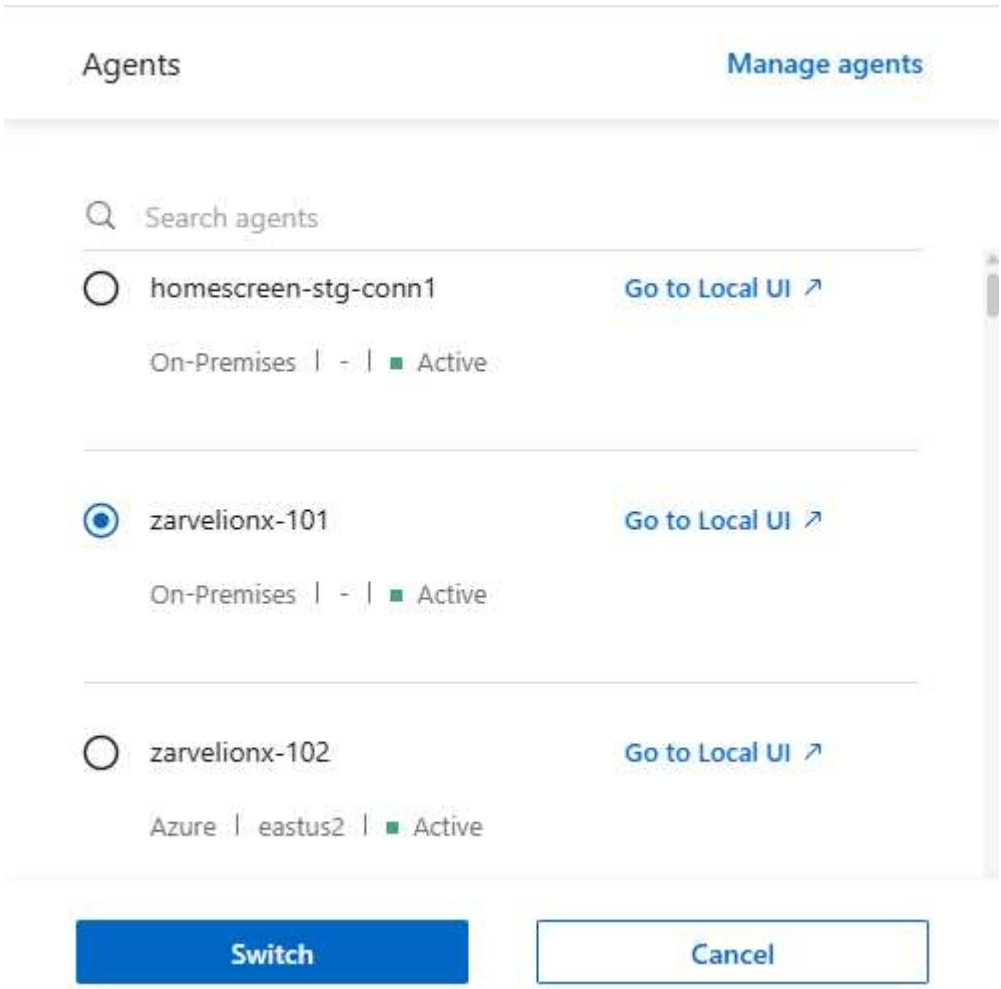
複数のコンソール エージェントがある場合は、それらを切り替えて、特定のエージェントに関連付けられているシステムを表示できます。

たとえば、マルチクラウド環境では、AWS にエージェントが 1 つあり、Google Cloud に別のエージェントがある場合があります。これらのエージェントを切り替えて、それぞれのクラウド環境内のCloud Volumes ONTAPシステムを管理します。

このオプションは、エージェントのローカル UI からNetApp Consoleを表示するときには使用できません。

手順

1. コンソールエージェントアイコン（ ）をクリックすると、利用可能なエージェントのリストが表示されます。



結果

コンソールが更新され、選択したエージェントに関連付けられているシステムが表示されます。

NetApp Consoleのホームページでメトリックを表示する

ストレージ資産の健全性を監視することで、ストレージ保護に関する問題を認識し、解決するための手順を実行できるようになります。 NetApp Consoleのホーム ページを使用して、 NetApp Backup and Recoveryからのバックアップとリストアのステータスと、 NetApp Ransomware Resilienceによって示されるようにランサムウェア攻撃のリスクがあるワークロードや保護されているワークロードの数を表示します。個々のクラスターとCloud Volumes ONTAPのストレージ容量、 ONTAPアラート、クラスターまたはCloud Volumes ONTAPシステムごとのストレージ パフォーマンス容量、保有しているさまざまな種類のライセンスなどを確認できます。

ホーム ページのすべてのペインには、組織レベルのデータが表示されます。ストレージ容量とストレージ パフォーマンス ペインには、IAM 権限に基づいてユーザーがアクセスできるプロジェクトに関連付けられたシステムが表示されます。

システムは、ホームページのデータを 5 分ごとに更新します。キャッシュにより、このページのデータが実際の値と最大 15 分間異なる可能性があります。

ホーム ページで正確なメトリックを得るには、適切なサイズと構成のコンソール エージェントが必要です。

必要なNetApp Consoleのロール

ホーム ページの各ペインには、異なるユーザー ロールが必要です。

- ストレージ容量ペイン: NetApp Consoleシステムページを表示する機能
- * ONTAPアラート ペイン*: フォルダまたはプロジェクト管理者、運用サポート アナリスト、組織管理者、組織閲覧者、スーパー管理者、スーパー閲覧者
- ストレージパフォーマンス容量ペイン: NetApp Consoleシステムページを表示する機能
- **Licenses and subscriptions**ペイン: フォルダーまたはプロジェクト管理者、組織管理者、組織閲覧者、スーパー管理者、スーパー閲覧者
- ランサムウェア耐性ペイン: フォルダまたはプロジェクト管理者、組織管理者、ランサムウェア耐性管理者、ランサムウェア耐性閲覧者、スーパー管理者、スーパー閲覧者
- バックアップとリカバリ ペイン: バックアップとリカバリ バックアップ管理者、バックアップとリカバリ スーパー管理者、バックアップとリカバリ バックアップ ビューアー、バックアップとリカバリ クローン管理者、フォルダーまたはプロジェクト管理者、組織管理者、バックアップとリカバリ リストア管理者、スーパー管理者、スーパー ビューアー

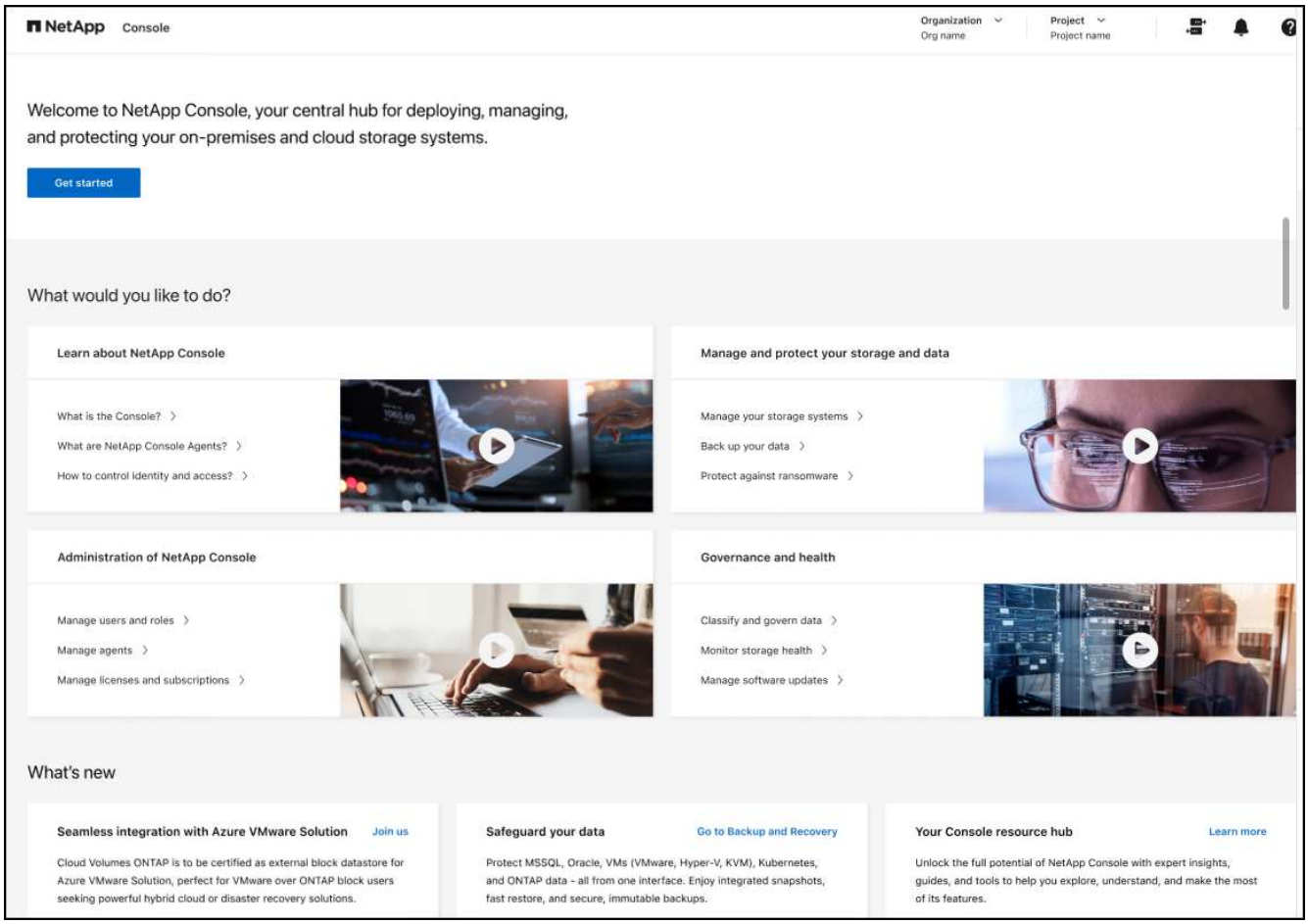
ペインにアクセスする権限がない場合は、そのペインを使用する権限がないことを示すメッセージが表示されます。

"NetApp Consoleのアクセス ロールについて学習します。" 。

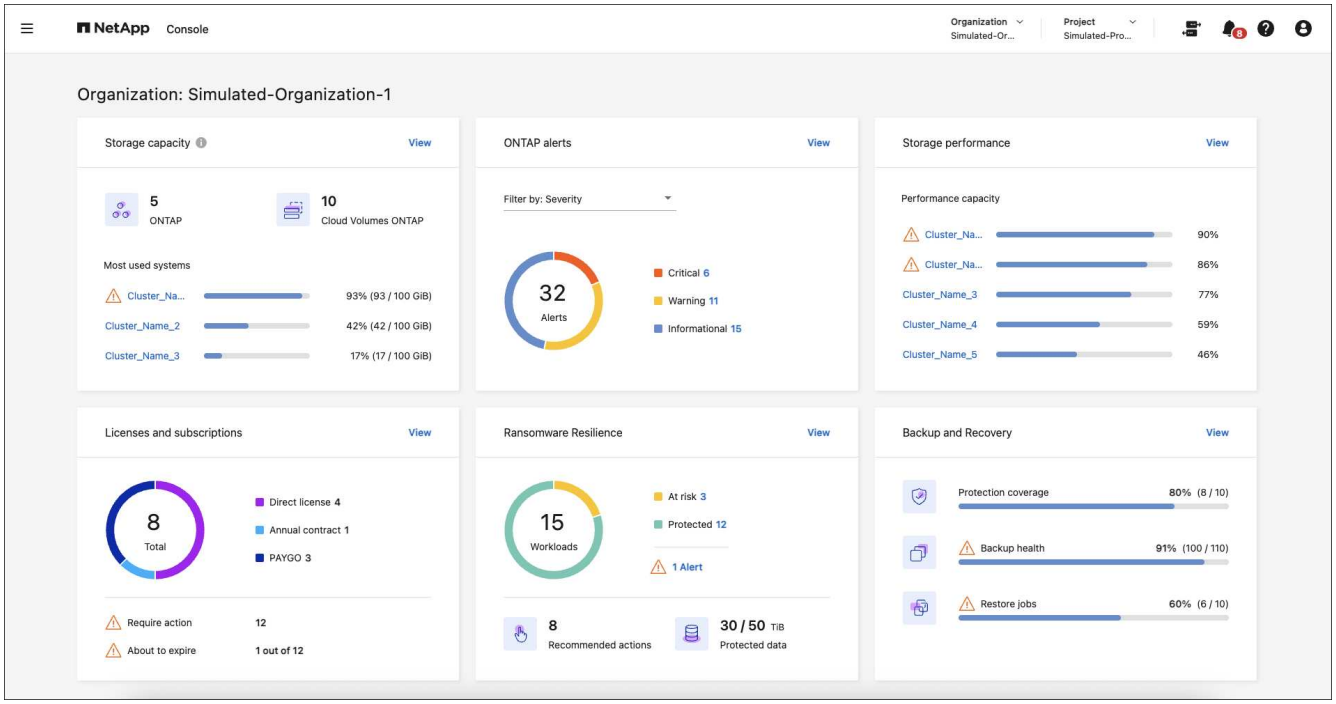
手順

1. NetApp Consoleメニューから、[ホーム] を選択します。

   組織管理者のロールがあり、エージェントまたはストレージ システムが設定されていない場合は、ホーム ページに開始方法の情報が表示されます。



   NetApp Consoleがすでに設定されていて、少なくとも 1 つのコンソール エージェントが有効になっていて、そのエージェントに少なくとも 1 つのクラスタまたはCloud Volumes ONTAPシステムが追加されている場合は、ホーム ページにストレージ環境に関するメトリックが表示されます。



ホーム ページに指標が表示されるようにする

次の条件が満たされると、ホーム ページでメトリックを表示できます。

- NetApp Consoleの SaaS インスタンスにログインしています。
- 既存のストレージ リソース (エージェントとクラスター、またはCloud Volumes ONTAPシステム) を持つ組織に属している。
- 少なくとも 1 つのコンソール エージェントが有効になっています。
- そのエージェントに少なくとも 1 つのクラスターまたはCloud Volumes ONTAPシステムが追加されています。

ホーム ページにメトリックが表示されるようにするには、次のタスクを実行します。

- 少なくとも 1 つのコンソール エージェントを有効にします。
- そのエージェントを使用して、少なくとも 1 つのクラスターまたは 1 つのCloud Volumes ONTAP を追加します。

全体のストレージ容量を表示する

ストレージ容量ペインには、 ONTAPクラスターとCloud Volumes ONTAPシステム全体の次の情報が表示されます。

- コンソールで検出されたONTAPシステムの数
- コンソールで検出されたCloud Volumes ONTAPシステムの数
- クラスターあたりの容量使用量

クラスターまたはCloud Volumes ONTAPシステムの順序は、使用される容量の量に基づいています。簡単に識別できるように、容量が最も大きいクラスターまたはシステムが最初に表示されます。

クラスターの容量が 80% になると警告インジケーターが表示され、データは 5 分ごとに更新されます。

> 複数のプロジェクトがある場合、システム ページと比較して、ストレージ容量ペインに異なるデータが表示されることがあります。これは、システム ページにはプロジェクト レベルに基づいて情報が表示されるのに対し、ストレージ容量ペインには組織レベルの情報が表示されるためです。また、パフォーマンスを最適化するためにデータがその期間キャッシュされるため、このペインのデータは最大 15 分間、実際の値と異なる場合があります。

手順

1. NetApp Consoleメニューから、ストレージ容量ペインを確認します。
2. ストレージ容量ペインで、表示 を選択して、コンソール システム ページに移動します。
3. 「システム」ページで、表示するクラスターを含むプロジェクトを選択します。
4. 「システム」ページでクラスターを選択すると、そのクラスターの詳細が表示されます。

ONTAPアラートを表示する

NetAppオンプレミスONTAP環境における問題または潜在的なリスクを表示します。 EMS 以外のアラートとEMS アラートがいくつか表示されます。

データは5分ごとに更新されます。

次の重大度のONTAPアラートが表示されます。

- 致命的
- 警告
- 情報

次の影響領域に関するONTAPアラートを確認できます。

- 容量
- パフォーマンス
- 保護
- 可用性
- セキュリティ

> キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

サポートされているシステム

- オンプレミスのONTAP NAS または SAN システムがサポートされています。
- Cloud Volumes ONTAPシステムはサポートされていません。

サポートされているデータソース

ONTAPで発生する特定のイベントに関するアラートを表示します。これらは、EMS とメトリックベースのア

ラートの組み合わせです。

ONTAPアラートの詳細については、 "ONTAPアラートについて" 。

表示される可能性のあるアラートのリストについては、以下を参照してください。 "ONTAPストレージの潜在的なリスクを表示する" 。

手順

1. NetApp Consoleメニューから、 ONTAPアラート ペインを確認します。
2. 必要に応じて、重大度レベルを選択してアラートをフィルタリングするか、影響領域に基づいてアラートを表示するようにフィルターを変更します。
3. ONTAPアラート ペインで [表示] を選択して、コンソール アラート ページに移動します。

ストレージパフォーマンス容量を表示

クラスターまたはCloud Volumes ONTAPシステムごとに使用されているストレージ パフォーマンス容量を確認し、パフォーマンス容量、レイテンシ、および IOPS がワークロードにどのような影響を与えているかを判断します。たとえば、重要なワークロードのレイテンシを最小限に抑え、IOPS とスループットを最大化するために、ワークロードをシフトする必要があることがわかる場合があります。

システムは、クラスターとシステムをパフォーマンス容量別に整理し、簡単に識別できるように、最も容量が大きいものを最初にリストします。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大 15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、ストレージ パフォーマンス ペインを確認します。
2. ストレージ パフォーマンス ペインで [表示] を選択すると、パフォーマンス容量、IOPS、レイテンシに関するすべてのクラスターとCloud Volumes ONTAPシステム データが一覧表示される [パフォーマンス] ページに移動します。
3. クラスターを選択すると、System Manager でその詳細が表示されます。

所有しているライセンスとサブスクリプションを表示する

[Licenses and subscriptions]ペインで次の情報を確認します。

- 保有しているライセンスとサブスクリプションの合計数。
- 保有しているライセンスおよびサブスクリプションの種類ごとの数 (直接ライセンス、年間契約、または PAYGO)。
- アクティブ、アクションが必要、または有効期限が近づいているライセンスとサブスクリプションの数。
- システムは、アクションが必要なライセンス タイプまたは有効期限が近づいているライセンス タイプの横にインジケーターを表示します。

データは5分ごとに更新されます。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、 [Licenses and subscriptions]ペインを確認します。
2. [Licenses and subscriptions]ペインで [表示] を選択して、コンソールの[Licenses and subscriptions]ページに移動します。

ランサムウェア耐性ステータスの表示

NetApp Ransomware Resilienceデータ サービスを使用して、ワークロードがランサムウェア攻撃のリスクにさらされているかどうか、または保護されているかどうかを確認します。保護されているデータの合計量を確認したり、推奨されるアクションの数を表示したり、ランサムウェア保護に関連するアラートの数を表示したりできます。

データは 5 分ごとに更新され、 NetApp Ransomware Resilience Dashboard に表示されるデータと一致します。

"NetApp Ransomware Resilienceについて学ぶ" 。

手順

1. NetApp Consoleメニューから、ランサムウェア耐性ペインを確認します。
2. ランサムウェア耐性ペインで次のいずれかを実行します。
   - 表示 を選択して、 NetApp Ransomware Resilienceダッシュボードに移動します。詳細については、"NetApp Ransomware Resilienceダッシュボードを使用してワークロードの健全性を監視する" 。
   - NetApp Ransomware Resilienceダッシュボードの「推奨アクション」を確認します。詳細については、 "NetApp Ransomware Resilienceダッシュボードで保護推奨事項を確認する" 。
   - アラート リンクを選択して、 NetApp Ransomware Resilience Alerts ページでアラートを確認します。詳細については、 "NetApp Ransomware Resilienceで検出されたランサムウェアアラートを処理する" 。

バックアップとリカバリのステータスを表示する

NetApp Backup and Recoveryからのバックアップと復元の全体的なステータスを確認します。保護されているリソースと保護されていないリソースの数を確認できます。ワークロードの保護のためのバックアップと復元操作の割合を確認することもできます。パーセンテージが高いほど、データ保護が強化されていることを示します。

データは5分ごとに更新されます。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、[バックアップとリカバリ] ペインを確認します。
2. 表示 を選択して、 NetApp Backup and Recoveryダッシュボードに移動します。詳細については、"NetApp Backup and Recoveryのドキュメント" 。

NetApp Consoleのユーザー設定を管理する

パスワードの変更、多要素認証 (MFA) の有効化、コンソール管理者の確認など、コンソール プロファイルを変更できます。

コンソール内では、各ユーザーにはユーザーとその設定に関する情報が含まれるプロファイルがあります。プロフィール設定を表示および編集できます。

表示名を変更する

他のユーザーが自分を識別するためのコンソールの表示名を変更できます。ユーザー名またはメールアドレスを変更することはできません。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 名前の横にある*編集*アイコンを選択します。
3. 名前 フィールドに新しい表示名を入力します。

読み取り専用モードで役割を高める

場合によっては、組織管理者が組織を読み取り専用モードに設定することがあります。管理者ロールを持っている場合は、変更を加えるために権限を昇格する必要があります。これにより、変更が意図的かつ承認されたものであることが保証されます。

役割を昇格した後は、現在のセッションの有効期限が切れるまでコンソールで変更を加えることができます。

完了したら、コンソールからログアウトするか、スライダーを戻して読み取り専用モードに戻ります。セッションの有効期限が切れると、システムによって昇格された権限が削除されます。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. *読み取り専用モードのステータス*については、スライダーを*昇格*の位置に移動し、変更を確認します。

多要素認証を設定する

2 番目の検証方法を必須にしてセキュリティを強化するには、多要素認証 (MFA) を構成します。

外部 ID プロバイダーまたはNetApp Support Siteでシングル サインオンを使用するユーザーは、MFA を有効にできません。これらのいずれかに該当する場合、プロフィール設定に MFA を有効にするオプションは表示されません。

ユーザー アカウントが API アクセスに使用されている場合は、MFA を有効にしないでください。ユーザー アカウントに対して多要素認証を有効にすると、API アクセスが停止されます。すべての API アクセスにサービ

ス アカウントを使用します。

開始する前に

- Google Authenticator や Microsoft Authenticator などの認証アプリをデバイスにダウンロードしておく必要があります。
- MFA を設定するにはパスワードが必要です。

> 認証アプリにアクセスできない場合、または回復コードを紛失した場合は、コンソール管理者に問い合わせてください。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. *多要素認証*ヘッダーの横にある*構成*を選択します。
3. 指示に従ってアカウントの MFA を設定します。
4. 完了すると、リカバリコードを保存するように求められます。コードをコピーするか、コードを含むテキスト ファイルをダウンロードするかを選択します。このコードを安全な場所に保管してください。認証アプリにアクセスできなくなった場合は、回復コードが必要になります。

   MFA を設定すると、コンソールにログインするたびに、認証アプリからのワンタイム コードを入力するように求められます。

MFA回復コードを再生成する

リカバリコードは 1 回のみ使用できます。使用済みまたは紛失した場合は、新しいものを作成してください。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 選択 ••• *多要素認証*ヘッダーの横。
3. *リカバリコードの再生成*を選択します。
4. 生成されたリカバリコードをコピーし、安全な場所に保存します。

MFA設定を削除する

完了したら、コンソールからログアウトするか、スライダーを戻して読み取り専用モードに戻ります。セッションの有効期限が切れると、システムによって昇格された権限が削除されます。

> 認証アプリまたは回復コードにアクセスできない場合は、組織の管理者に連絡して MFA 構成をリセットする必要があります。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 選択 ••• *多要素認証*ヘッダーの横。
3. *削除*を選択します。

組織管理者にお問い合わせください

組織の管理者に連絡する必要がある場合は、コンソールから直接メールを送信できます。管理者は、組織内のユーザー アカウントと権限を管理します。

*管理者に連絡*機能を使用するには、ブラウザにデフォルトの電子メール アプリケーションが設定されている必要があります。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 組織の管理者にメールを送信するには、[管理者に連絡] を選択します。
3. 使用する電子メール アプリケーションを選択します。
4. メールを終了し、[送信] を選択します。

ダークモード（ダークテーマ）を設定する

コンソールをダークモードで表示するように設定できます。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. ダーク テーマ スライダーを動かして有効にします。

著作権に関する情報

商標に関する情報