NetApp Console
ローカルデプロイメントドキュメント
NetApp Console local deployment

NetApp
August 10, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/console-local/index.html on August 10, 2026.
Always check docs.netapp.com for the latest.

目次

NetApp Console ローカル展開

リリース ノート

NetApp Console ローカル展開の最新情報

NetApp Console ローカル展開の最新リリースにおける新機能と強化点について説明します。

NetApp Consoleローカル デプロイのご紹介

"NetApp Console ローカル展開について学ぶ"。

NetApp Console ローカル展開における既知の制限事項

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しないプラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

これらの制限は、NetApp Consoleと管理のセットアップに固有のものです：エージェント、サービスとしてのソフトウェア（SaaS）プラットフォームなど。

コンソールVMの制限

10.42.0.0/16および10.43.0.0/16の範囲のIPアドレスとの競合の可能性

NetApp Consoleのローカル展開では、サービス間通信に固定アドレス空間が使用されます。内部ネットワークには、IPアドレス範囲10.42.0.0/16と10.43.0.0/16が使用されます。Console のローカル展開を展開する前に、これらのIPアドレス範囲が、Console のローカル展開で使用可能なVLAN上の他のVM、DHCPスコープ、DNSレコード、またはロードバランサーのVIPプールに割り当てられていないことを確認してください。

エージェントのインターフェースのIPアドレスを変更する方法については、ナレッジベースの記事「Agent IP conflict with existing network」を参照してください。

共有Linuxホストはサポートされていません

このエージェントは、他のアプリケーションと共有されている仮想マシンではサポートされていません。その仮想マシンはエージェントソフトウェア専用にする必要があります。

サードパーティのエージェントと拡張機能

サードパーティ製のエージェントやVM拡張機能は、エージェントVMではサポートされていません。

NetApp Console ローカル展開と NetApp Console の比較

クラウドとオンプレミス環境を管理し、プラットフォームインフラストラクチャを NetApp に任せたい場合は、NetApp Console を選択してください。大規模なオンプレミス ONTAP 環境を管理し、完全なデータ主権とポリシーベースのストレージ管理が必要な場合は、NetApp Console ローカル展開を選択してください。

NetApp Console

NetAppは、NetApp ConsoleをSaaSアプリケーションとしてホストおよびメンテナンスします。登録後すぐにストレージの管理を開始できます。ストレージシステムを管理するには、クラウドまたはオンプレミス環境に軽量のコンソールエージェントをデプロイします。エージェントはNetApp Consoleプラットフォームにアウトバウンド接続し、NetAppがプラットフォームの認証、アップグレード、および可用性を自動的に処理します。

NetApp Console は、制限モード（独自のパブリッククラウドにインストールされ、アウトバウンド接続が制限されている）とプライベートモード（オンプレミスまたはクラウドにインストールされ、エアギャップ環境を含む NetApp Console プラットフォームへの接続がない）もサポートしています。

"NetApp Console の導入モードについて"。

NetApp Consoleは、Amazon FSx for ONTAP、Cloud Volumes ONTAP、Amazon S3、Google Cloud Storage、Eシリーズ、StorageGRID、オンプレミスONTAPクラスターなどのクラウドストレージを含む、幅広いストレージシステムをサポートしています。NetApp Backup and Recovery、NetApp Disaster Recovery、NetApp Ransomware Resilience、NetApp Copy and Sync、NetApp Data Classificationなど、NetAppデータサービスのフルスイートへのアクセスを提供します。NetApp Consoleは、Digital Advisor、ライフサイクルプランニング、サステナビリティダッシュボードなどのサポート契約機能も提供しています。

NetApp Consoleは、ハイブリッドクラウド環境を管理し、最大限の機能、運用維持の手間軽減、そして柔軟なライセンス体系を求める組織に最適です。

"NetApp Console^について説明します。"

NetApp Console ローカル展開

NetApp Console のローカル展開では、NetApp Console のコントロールプレーンをお客様自身のオンプレミスインフラストラクチャ内で完全に実行でき、管理トラフィックが環境外に流出することはありません。仮想アプライアンスイメージを使用してコンソールを仮想マシンとしてデプロイし、vCenter環境内の他の仮想マシンと同様に管理します。コンソールエージェントは不要です。仮想マシンは、お客様の ONTAP クラスターと直接通信します。

NetApp Console のプライベートモードはエアギャップおよびオンプレミスデプロイメントもサポートしていますが、Console ローカルデプロイメントは、エンタープライズ規模の ONTAP フリート管理に特化して設計されています。これは、どの NetApp Console デプロイメントモードでも利用できない機能を追加するものです：

ストレージクラスポリシー

パフォーマンス、容量、階層化の要件をまとめた再利用可能なテンプレートとして、ストレージ標準を一度定義します。すべてのプロビジョニングは承認済みのクラスを使用し、Console のローカル展開はワークロードのコンプライアンスを継続的に監視し、ドリフトを特定します。

フリート管理

ビジネス構造を反映したフォルダとフリートにクラスターを整理し、組織、フォルダ、またはフリートのスコープで管理を委任します。

ワークロードアナライザー

レイテンシ、スループット、1秒あたりの入出力操作数、および構成変更を時系列で相関させることで、ワークロードに影響が出る前にパフォーマンスの問題を特定します。

大規模言語モデル統合

独自の大規模言語モデルに接続することで、自然言語を使用してストレージをプロビジョニングしたり、アラートを調査したり、ストレージ環境に関する状況に応じた回答を取得したりできます。

ガイド付きおよび自動化された修復

ワークロードがストレージクラスから逸脱したり、アラートが発生したりした場合、Console のローカル展開では修正推奨事項が提供されます。ガイド付き手順またはワンクリック自動修復機能を使用して、手動操作なしでコンプライアンスを回復できます。

メールとウェブフックによるアラート配信

保管状況が変化した際に、適切なチームにアラートが届くように、メールとWebhookの通知チャネルを設定してください。Webhookは、既存の監視ツールやインシデント管理ツールと連携します。

コンソールのローカル展開は、オンプレミス ONTAP クラスターと NetApp Backup and Recovery をサポートしています。Active Directory と連携してフェデレーション認証を実現し、ローカルユーザー向けの多要素認証もサポートしています。

コンソールローカル展開は、ポリシーベースのプロビジョニング、自動コンプライアンスチェック、および完全なデータ主権を必要とする大規模なオンプレミス ONTAP 環境を持つ組織に最適です。

"NetApp Console のローカルデプロイメントについて説明します^。"

機能比較

ストレージ管理

機能	**NetApp Console**	**NetApp Console** ローカル展開
オンプレミス ONTAP クラスター	はい（Console エージェントが必要です）	はい（コンソール仮想マシンからの直接通信）
クラウドストレージシステム（Amazon FSx for ONTAP、Cloud Volumes ONTAP 、Amazon S3、およびその他）	はい	×
EシリーズとStorageGRID	はい	×
NetApp Backup and Recovery	はい	はい
NetApp Disaster Recovery	はい	×
NetApp ランサムウェア耐性	はい	×
NetApp Copy and Sync	はい	×
NetApp データ分類	はい	×
Digital Advisor、Lifecycle Planning 、Sustainability	はい	×

機能	**NetApp Console**	**NetApp Console** ローカル展開
ストレージクラスポリシーとコンプライアンス監視	×	はい
ガイド付きおよび自動化された修復	×	はい
フリート管理（フォルダとフリート）	×	はい
ワークロードアナライザー	×	はい
AI支援オペレーションのための大規模言語モデルの統合	×	はい

コンソールの設定とセキュリティ

機能	**NetApp Console**	**NetApp Console** ローカル展開
展開モデル	NetAppがホストするSoftware as a Service（さまざまなデプロイモードを利用可能）	自社インフラストラクチャ内でホストされる仮想マシン
コンソールエージェントが必要です	はい	×
ソフトウェアのアップグレード	NetAppによる自動管理	手動
ユーザーインターフェースへのアクセス	NetApp Consoleアプリケーション（インターネットまたは仮想マシンからのアクセス）	コンソール仮想マシン（ローカル、インターネット不要）
データ主権	管理トラフィックはNetApp Consoleプラットフォームに送られます	データや管理トラフィックがお客様の環境から外部に出ることはありません。
Active Directoryとの統合	×	はい
アイデンティティフェデレーション	はい	×
多要素認証（ローカルユーザ）	はい	はい
監査ロギング	はい	はい
ライセンス	マーケットプレイスのサブスクリプションとライセンス持ち込み	ライセンス持ち込み（BYOL）

はじめに

NetApp Console のローカル展開について

NetApp Console のローカル展開では、お客様独自のインフラストラクチャで NetApp Console の自律コントロールプレーンをホストして実行できます。

統合ストレージ管理、ポリシー適用、フリート規模の自動化、AI支援による運用を実現します。データ、メタデータ、管理トラフィックは、お客様の環境外には一切送信されません。

独自のインフラストラクチャに **Console** をデプロイして運用する

NetApp Console ローカルデプロイメントは、お客様自身のインフラストラクチャ内で実行されるため、お客様のチームがデプロイメント、接続性、および日常的な運用を管理できます。Console エージェントをデプロイし、Console 仮想マシンを維持管理し、監視および管理トラフィックに必要なネットワークパスを管理します。これにより、企業管理者は運用境界を完全に制御しながら、管理データを環境内に保持できます。

- "vCenterでOVAを使用してNetApp Consoleのローカルデプロイをインストールします".
- "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".
- "オンプレミス Console エージェントのポートについては、NetApp Console ローカル展開を参照してください".

APIとサービスアカウントを使用してストレージ操作を自動化する

NetApp Console のローカル展開は API ベースの統合をサポートしているため、組織は反復可能なストレージ操作を自動化できます。サービスアカウントを使用すると、アプリケーションは割り当てられたロールで認証および操作を行うことができます。インタラクティブユーザーに適用されるものと同じロールベースのアクセス制御および監査制御が、これらの操作を管理します。これにより、アクセス範囲を限定して説明責任を維持しながら、エンタープライズの自動化を支援します。

- "メンバーを NetApp Console ローカル展開組織に追加する".
- "NetApp Console IAM の API について"

RBACと**Active Directory**の統合によるアクセス制御

NetApp Console のローカル展開は、ユーザーが管理するフリートやリソース内でユーザーが参照・実行できる内容を制限する、ゼロトラストのロールベースアクセス制御（RBAC）を提供します。Active Directory と統合することで、ユーザーは既存の企業認証情報でサインインできるようになり、ローカルユーザーは多要素認証（MFA）を追加してさらなる検証レイヤーを設けることができます。アクセスガバナンスは、組織の幅広いアイデンティティおよびアクセス管理の実践と整合性を保ちます。

- "NetApp Console ローカル展開におけるアイデンティティとアクセス管理について".
- "NetApp Console ローカル展開への安全なアクセスについて".

フリートを整理してストレージ管理を委任する

NetApp Console のローカル展開では、リソースをフォルダとフリートに整理することで、管理の拡張性を高めます。フリートを環境、事業部門、または地域にマッピングし、組織、フォルダ、またはフリートのスコープで管理を委任することで、所有権を明確に保つことができます。この構造により、大規模なストレージチームは、ポリシーの一貫性やガバナンスを損なうことなく、作業を分散させることができます。

- "NetApp Console ローカル展開におけるフォルダーとフリートについて".
- "NetApp Console ローカル展開のストレージフリートについて".

コンプライアンスのために管理活動を追跡およびエクスポートする

すべての管理操作は監査レコードを生成します。セキュリティおよびコンプライアンスチームは、これらのレコードを利用して、インシデントの調査、統制の有効性の証明、および監査要件への対応を行うことができます。集中監視、長期保存、および分析のために、Webhookを介して syslog サーバーに監査ログをエクスポートします。NetApp Console のローカルデプロイメントはお客様自身の環境で実行されるため、ログデータが

お客様のインフラストラクチャの外部に送信されることはありません。

- "NetApp Consoleのローカル デプロイ アクティビティの監査".

ストレージクラスポリシーに従ってストレージを一貫してプロビジョニングする

NetApp Console のローカル展開では、ストレージクラス（パフォーマンス、容量、階層化ポリシーを再利用可能な定義にまとめたテンプレート）を通じて、一貫したストレージ動作が適用されます。管理者はストレージ基準を一度定義します。管理者と自動化されたワークフローは、承認されたクラスを使用して、環境全体におけるすべてのプロビジョニング活動を実行します。これにより、構成のずれを防ぎ、経験の浅い管理者がプロビジョニングの決定に費やす時間を短縮し、すべてのワークロードが組織の基準を即座に満たすことが保証されます。プロビジョニング後、Console のローカル展開は、各ワークロードのコンプライアンスを継続的に監視します。

- "NetApp Console ローカル展開によるストレージ管理について".

ストレージクラスのコンプライアンスを監視し、ドリフトを自動的に修復します

NetApp Console のローカルデプロイメントは、プロビジョニングに使用されたストレージクラスに対して、すべてのワークロードを監視します。ワークロードが、クラスタ構成の直接的な変更やパフォーマンスの低下によって変動する場合、NetApp Console のローカルデプロイメントは違反を即座に検出します。管理者は、ガイド付きの修復手順に従うか、自動修復を設定することで、手動による介入なしに一般的なドリフト状態を解決できます。この継続的な実施により、監査リスクが軽減され、定期監査の間も環境がコンプライアンス状態を維持できます。

ストレージの状態を監視し、複数のフリートにわたるアラートを受信する

NetApp Console のローカルデプロイメントでは、管理するすべてのクラスターの状態とパフォーマンスを単一の場所で監視できます。フリート全体のダッシュボードには、注意が必要なクラスターとボリュームが表示されます。カスタムダッシュボードを使用すると、管理者は自身の責任範囲に合った監視ビューを作成できます。ワークロードアナライザーは、レイテンシ、スループット、リソース使用率、構成変更を時系列で相関分析し、問題がワークロードに影響を与える前に根本原因を特定するのに役立ちます。

状況が変化した際に適切なチームにアラートが届くよう、メールとWebhookの配信チャネルを設定してください。組織管理者が宛先を設定し、ストレージ管理者がアラートルールにそれらを適用することで、応答パスが運用モデルに一致するようにします。これにより、企業チームは容量、パフォーマンス、および保護に関するイベントに迅速に対応できるようになります。

- "NetApp Console ローカル展開におけるストレージの健全性監視について".
- "NetApp Console ローカル展開で通知配信チャネルを設定する".
- "NetApp Console ローカル展開でアラートの通知ルールを設定する".

自然言語でストレージをプロビジョニングし、アラートを調査する

NetApp Console ローカル展開では、独自の大規模言語モデル（LLM）に接続して、AI支援によるストレージ管理を提供できます。ワークロードを平易な言葉で説明することで、プロビジョニングプランを取得したり、Console にアクティブなアラートの調査を依頼したり、ストレージ環境に関する状況に応じた回答を得たりすることができます。すべての AI アクションは、ストレージクラスのガードレールおよびお客様のアカウントに適用されるロールベースのアクセス制御の範囲内に留まり、機密性の高い操作を実行する前に確認が必要です。Console ローカル展開では、管理者が設定した LLM エンドポイントにのみリクエストが送信されます。

- "NetApp Console ローカル展開における LLM 統合について".

NetApp Backup and Recoveryを使用したストレージのバックアップとリストア

プロビジョニングとモニタリングにとどまらず、NetApp Console のローカル展開により NetApp Backup and Recovery へのアクセスが可能になり、同じインターフェースからデータを保護できます。データのバックアップとリストアを実行することで、保護とリカバリの要件を満たすことができます。ストレージと並行してデータ保護を管理することで、ガバナンスの一貫性が保たれ、チームが業務を遂行するために必要なツールの数を削減できます。

- "NetApp Console ローカル展開のデータサービスについて".

NetApp Console ローカル展開のIDとアクセス管理について

NetApp Consoleのローカル展開におけるIDとアクセス管理（IAM）では、サインインできるユーザー、IDの検証方法、ユーザーがアクセスできるリソース、およびユーザーが実行できるアクションを制御します。NetApp Consoleのローカル展開において、IAMには、ロールベースのアクセス制御（RBAC）、多要素認証（MFA）、ディレクトリベースの認証のほか、委任管理をサポートする階層モデルおよび監査モデルが含まれます。

このページでは、NetApp Console のローカル展開における IAM モデルの概要を説明します。詳細な階層計画の例については、"NetApp Console ローカル展開におけるフォルダーとフリートについて"。

NetApp Console で IAM を管理するには、スーパー管理者、組織管理者、または フォルダーまたはフリート管理者 のロールが必要です。

IAMが**NetApp Console**のローカル展開において意味すること

NetApp Console ローカル展開 IAM は、ID 検証、アクセス制御、委任、および監査可能性を統合します：

- 認証は、ユーザーがローカルの認証情報を使用するか、ディレクトリ構成を通じてサインインするかを決定します。
- _認可_は、事前に定義されたロールと、それらを割り当てるスコープに基づいて、メンバーがサインイン後に実行できる操作を決定します。
- 階層とスコープによって、メンバーがアクセスできるフォルダー、フリート、およびリソースが決まります。
- _メンバーと認証情報の管理_では、ユーザーやサービスアカウントを追加する方法、およびMFAとサービスアカウントのシークレットを管理する方法を決定します。
- _監査およびコンプライアンス追跡_は、IAM関連のアクティビティを記録するため、誰がいつアクセス権限を変更したかを確認できます。

認証の仕組み

NetApp Console のローカル展開は、ローカル ID と外部 ID 統合の両方をサポートしています。

NetApp Consoleのローカル展開をActive Directoryと統合することで、ユーザーは既存の企業の資格情報を使用してサインインできるようになります。これにより、Consoleのローカル展開で個別のパスワードを使用する必要がなくなり、管理者はアクセス権を割り当てる際にディレクトリユーザーを検索できるようになります。

ローカルユーザーの場合、MFA は認証情報が漏洩した場合の不正アクセスリスクを軽減するために、追加の認証手順を追加します。

認証と安全なサインインオプションの詳細については、"NetApp Consoleのローカル デプロイにおけるセキュア アクセスについて説明します"。

認可の仕組み

ユーザーがサインインした後、NetApp Console のローカル展開では、RBAC を使用して、そのユーザーが何を表示および実行できるかを決定します。

認証はActive DirectoryまたはLDAPとの連携によって処理されます。NetApp Consoleのローカル展開における認可は別個のものであり、管理者は組織、フォルダ、またはフリートレベルで事前定義されたロールを割り当てて、各メンバーがアクセスできる内容を制御します。

同じロールであっても、割り当てるスコープによって有効なアクセス権限は異なります。このモデルでは、中央管理者には広範なアクセス権限を付与しつつ、地域管理者やチームレベルの管理者にはそれぞれが管理するフリートへのアクセス権限を制限できます。

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、子スコープに継承されます。この継承モデルは、NetApp Console がフォルダとフリート間でアクセス権を委任する方法の重要な部分です。

NetApp は、最小権限の原則に基づいて NetApp Console のローカル展開ロールを設計しており、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。

"NetApp Console ローカル展開におけるロールベースのアクセス制御とロール継承について学ぶ".

IAM階層の仕組み

NetApp Console のローカル展開では、階層構造を使用してリソースをグループ化し、アクセス範囲を限定します。最上位に組織があり、その下にフォルダ、次にフリート、そしてそれらのフリートに関連付けられたリソース（サブフォルダを含む場合もあります）が続きます。

この階層構造こそが、権限委譲を可能にするものです。例えば、組織管理者は組織全体にわたるアクセスを管理できますが、フォルダ管理者やフリート管理者は、自身が所有する階層内のリソースとメンバーのみを管理できます。

NetApp Console IAMは、階層構造を定義する組織コンポーネント、その階層構造内に割り当てられるリソース、そして誰が何にアクセスできるかを制御するメンバーとロールという、3種類のコンポーネントに基づいて構築されています。

役割はこの階層を通じて継承されるため、フォルダとフリートの設計は、各アクセス割り当ての適用範囲に直接影響します。

"組織にフリートを追加する方法について説明します。".

メンバーのセキュリティと認証情報

NetApp Console のローカル展開における IAM には、アカウント作成後のメンバーアクセスを保護するための運用制御機能も含まれています。

ローカルユーザーの場合、管理者はパスワードのリセットを指示したり、MFAを削除または一時的に無効化したり、ローカルユーザーのMFAの動作を確認したりすることで、ユーザーのアクセス回復を支援できます。サ

ービスアカウントの場合、管理者はシークレットが紛失またはローテーションされた場合に認証情報を再作成できます。

これらの制御はIAMの一部です。これは、アクセス権限が最初にどのように割り当てられるかだけでなく、時間の経過とともにIDがどのように安全に維持されるかを決定するためです。

"メンバーのセキュリティを管理する方法を説明します".

IAMアクティビティの監査

NetApp Console のローカル展開における IAM には、アクセス関連のアクティビティを確認およびエクスポートする機能が含まれています。

監査ページからは、メンバーの追加、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を確認できます。また、監査記録をテナントサービスでフィルタリングしてIAM関連の変更に絞り込んだり、監査ログを外部システムにエクスポートしたりすることもできます。

監査可能性は、IAMの重要な原則です。なぜなら、誰がアクセス権限を変更したか、変更が行われた日時、そして変更が成功したかどうかを検証できるからです。

"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".

NetApp ConsoleでのIAMの次のステップ

- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "NetApp Consoleのローカル デプロイにおけるセキュア アクセスについて説明します"
- "NetApp Console ローカル展開における RBAC について"
- "コンソールのローカル展開アクティビティを監視または監査する"
- "NetApp Console IAM の API について"

NetApp Console ローカルデプロイにおけるフリート管理について説明します

NetApp Consoleのローカル展開におけるフリート管理とは、ストレージシステムを論理グループに整理することで、一貫したポリシーの適用、アクセス制御、および関連するクラスター全体のヘルス状態の監視を行うプラクティスです。フリート管理を使用すると、各クラスターを個別に管理する代わりに、フリートを共通のリソースプールとして扱い、データストレージの目標をサポートできます。

ストレージ環境が拡大するにつれて、個々のクラスターを管理することは非現実的になります。フリート管理は、関連するシステムを体系的にグループ化し、責任を委任し、すべてのクラスターが同じ基準で運用されるようにすることで、この問題を解決します。

フリート管理が重要な理由

フリート管理は、以下の3つの主要な課題に対処します：

- 抽象化による簡素化 - フリート管理は、個々のストレージインフラストラクチャの管理の複雑さを抽象化します。クラスターごとに設定を行う代わりに、ストレージ環境全体を統一的に管理することで、運用上の負担と意思決定の負担を軽減できます。

- 一貫性と拡張性 - 明確な組織体制がないと、異なるチームが類似のワークロードに対して異なる決定を下し、断片化された構成につながります。フリート管理機能を使用すると、数十ものシステムに同時に標準を適用できるため、新しいワークロードがチームやフリート全体で同じ基準から開始されることが保証されます。
- ガバナンスと管理 - チームが大きくなるにつれて、誰が何を管理できるかについて明確な境界線が必要になります。フリート管理は、組織構造とアクセス制御を通じてこれらの境界を設定し、ストレージに関する決定が統制され、監査可能であることを保証します。

フリートによるリソースの整理方法

組織のリソース階層は、フォルダーとフリートで構成されています。

階層構造とアクセスモデルの詳細については、"NetApp Console ローカル展開におけるフォルダーとフリートについて"を参照してください。

- 組織 - お客様の会社を表す最上位レベル。
- 「フォルダー」：関連するフリートを整理するのに役立ちます。たとえば、リージョンやビジネスユニットごとにフォルダーを作成し、各フォルダー内にフリートを作成できます。フォルダーには、他のフォルダーやフリートを含めることができます。フォルダーレベルでロールを割り当てると、メンバーはそのフォルダー内のすべてのフリートに対してそのロールを継承します。
- フリート - 管理しているストレージシステムをグループ化します。ストレージシステムをフリートに関連付け、メンバーをフリートに割り当てることでアクセス権を付与します。

フォルダは組織管理ツールであり、組織管理者、フォルダ管理者、フリート管理者などのIAM権限を持たないメンバーには表示されません。メンバーはフォルダではなく、フリートにアクセスします。

一般的なフリート編成パターン

フリートの編成方法は、運用モデルによって異なります。

- 環境別 - 本番環境、開発環境、テスト環境のワークロード用に個別のフリートを作成します。これにより、本番環境のストレージはより厳格なポリシーの下で管理される一方、下位環境ではより高い柔軟性が確保されます。
- 事業部門別 - 財務、エンジニアリング、人事など、特定の部門にサービスを提供するクラスターを専用のフリートにまとめます。そうすることで、他のフリートを公開することなく、その事業部門内のチームメンバーにストレージ管理の責任を割り当てることができます。
- 場所またはデータセンター別 - クラスターが複数のサイトに分散している場合、場所別に整理することで、サイトレベルの健全性を監視したり、地域固有のポリシーを適用したり、サイトごとの容量消費量を追跡したりできます。
- アプリケーション層別 - データベース、ファイル共有、仮想マシンなど、特定の種類のワークロードをホストするクラスターをグループ化することで、そのワークロードタイプに合わせて調整された一貫した標準をフリート全体に適用できます。

フォルダを使用して、さらに整理のレベルを追加します。例えば、地域ごとにフォルダを作成し、各地域フォルダ内に環境ベースのフリートを作成します。

フリート管理がアクセス制御を可能にする方法

フリートとフォルダは、ユーザーアクセスと管理責任の境界として機能します。

- フォルダレベルのアクセス - フォルダレベルで役割を割り当てると、メンバーはそのフォルダ内のすべてのフリートとリソースに対してその役割を継承します。これにより、組織全体へのアクセス権を付与することなく、管理上の責任を委任できます。
- フリートレベルのアクセス - フリートレベルで役割を割り当てると、メンバーはそのフリート内のストレージシステムにのみアクセスできます。これにより、インフラストラクチャの無関係な部分を公開することなく、ストレージ管理をチームメンバーやアプリケーション所有者に委任できます。

コンソールローカル展開では、フリートレベルの健全性とパフォーマンスの監視機能が提供されるため、フリート内のすべてのクラスターの状態を単一のビューで確認し、問題を早期に特定して、ワークロードに影響が出る前に対応できます。

ストレージ管理の仕組み

ストレージ管理とは、ストレージの標準を定義し、それを一貫して適用し、ワークロードが長期にわたって整合性を保つように運用する実践のことです。Console のローカル展開では、これらの標準はストレージクラスポリシーとストレージクラスとして表現され、フリートごとにスコープが設定され、RBAC と監査ログによって管理されるプロビジョニングワークフローを通じて適用されます。

コンソールローカル展開では、4つの概念が1つのワークフローに統合されます：

- *フリート*は、ストレージを管理する範囲を定義します。フリートとは、システムをグループ化することで、アクセスを制御し、標準を一貫して適用し、リソースを単位として管理できるようにするものです。
- *ストレージクラスポリシー*は、再利用可能な構成要素（パフォーマンス、容量、セキュリティ、データ保護）として標準を定義します。
- *ストレージクラス*はワークロードの意図を表します。ストレージクラスとは、1つ以上のポリシーから構成される、名前付きのテンプレートのことです。
- *プロビジョニングワークフロー*は、ガードレール内でストレージを作成します。ワークフローによって構成決定の方法は異なりますが、いずれの場合もストレージクラスを適用でき、RBACと監査ログによって管理されます。

プロビジョニングのアプローチ

コンソールのローカル展開では、3つのプロビジョニング方式がサポートされており、いずれもRBAC、監査ログ、およびストレージクラス標準によって管理されます。

- 手動プロビジョニング - 対象システムを選択し、構成の詳細を直接指定します。システム選択と構成を明示的に制御する必要がある場合に使用します。
- 自動プロビジョニング - ワークロードの入力値を指定し、必要に応じてストレージクラスを選択します。NetApp Console のローカル展開では、最適な配置が推奨され、クラス駆動型の設定が適用されるため、手動での決定が軽減されます。
- **AI**支援（エージェント型）プロビジョニング - 必要なものを自然言語で説明します。Console のローカル展開では、RBAC とストレージクラスによって制約されたプランが提案され、お客様が確認して承認した後にのみプロビジョニングが実行されます。

次のステップ

- ストレージ規格を理解するには、"NetApp Console ローカル展開におけるストレージクラスとポリシーについて"を参照してください。
- フリートの作成と管理については、"フォルダとフリートを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"
- "AI支援によるストレージの提供"

NetApp Console ローカル展開におけるストレージクラスとポリシーについて

ストレージクラスとは、ストレージがどのように動作するべきかを定義する、再利用可能なテンプレートです。ストレージクラスを使用してストレージをプロビジョニングする場合、NetApp Console のローカル展開では、管理者がワークロードごとに個別の構成決定を行う必要なく、そのクラスにエンコードされた標準が自動的に適用されます。

ストレージクラスは、ストレージ動作の個々の側面を定義するストレージクラスポリシーに基づいて構築されます。これらを組み合わせることで、組織のストレージ標準を一度設定すれば、それをすべてのシステムで一貫して適用できるようになります。

ストレージクラスポリシーとは

ストレージクラスポリシーは、ストレージの動作の一側面を定義します。ポリシーは、ストレージクラスを作成するために組み合わせる、再利用可能な構成要素です。

一般的なポリシーの種類は以下のとおりです：

- パフォーマンス ポリシー - レイテンシー ターゲット、IOPS、またはスループット要件を定義します。
- 容量ポリシー - プロビジョニングモード、しきい値アラート、または拡張制限を定義します。
- セキュリティポリシー - 暗号化、コンプライアンス、またはアクセス制御の要件を定義します。
- データ保護ポリシー - スナップショットのスケジュール、レプリケーションのターゲット、または保持期間を定義します。

ポリシーは個別に定義し、ストレージクラスを構築する際にそれらを組み合わせます。これにより、複数のクラスで同じパフォーマンス ポリシーを再利用したり、容量ポリシーを 1 か所で更新して、そのポリシーを使用するすべてのクラスにその変更を適用したりすることができます。

ストレージクラスとは

ストレージクラスとは、1つ以上のポリシーから構成される、名前付きのテンプレートのことです。これは、特定の種類のワークロードに対する組織のストレージ標準を表すものです。

例えば、ハイパフォーマンス、高可用性、厳格な保護ポリシーを組み合わせた **Production Database** ストレージクラス、または適度なパフォーマンス、柔軟な容量、基本的な保護ポリシーを組み合わせた **Development File Share** ストレージクラスを作成することができます。

ストレージ管理者は、企業要件を反映させるためにストレージクラスを定義します。プロビジョニング活動は、手動で行う場合でも、ガイド付きワークフローを通じて行う場合でも、自動化によって行う場合でも、管

理者が承認したクラスのライブラリからデータを取得します。

ストレージクラスが標準をどのように適用するか

ストレージをプロビジョニングする際は、個々の設定を構成するのではなく、ストレージクラスを選択します。Console のローカル展開では、そのクラスのポリシーを使用して、フリート内のどのクラスターがワークロードをサポートする容量とパフォーマンスの余裕を持っているかを特定し、最適な配置オプションを推奨し、プロビジョニング時にクラス駆動型の設定を自動的に適用します。

プロビジョニング後、NetApp Console のローカルデプロイメントは、各ワークロードをストレージクラスの標準に照らし合わせて継続的に評価します。

ストレージクラスの変更とコンプライアンス

ワークロードがストレージクラスの意図と一致しなくなった場合、Console のローカルデプロイメントは、調査と修復のためにそのワークロードにフラグを立てます。

問題は2つのカテゴリーに分類されます：

- 構成のずれ：ストレージクラスポリシーによって管理されるストレージ設定が、意図した構成と一致しなくなりました。これは、ONTAP クラスターで直接変更が行われた場合、または標準のプロビジョニングワークフロー外で変更が行われた場合に発生する可能性があります。
- パフォーマンス不適合：ワークロードの実行時動作がストレージクラスのパフォーマンス要件を満たさなくなりました（たとえば、QoS 制限付近での持続的な負荷、またはテールレイテンシの増加など）。

分析ビューでは、何が変わったのか、そしてなぜ変わったのかが説明されます。コンプライアンスを回復するために、ガイド付きの是正措置（例えば、**Fix it** など）が利用できる場合があります。一部の修復策はそのまま適用できますが、意図した動作を復元するためにワークロードを別のストレージクラスに調整する必要がある場合もあります。

調査する場所

通常、以下のいずれかの場所からドリフトやコンプライアンス違反を調査できます（利用可能かどうかは、デプロイメントと権限によって異なります）：

- ストレージクラス： ドリフト / コンプライアンス
- アラート： 分析

手順の詳細については、ストレージクラスのずれを修正するを参照してください。

エンドツーエンドのワークフロー

以下の手順では、ストレージクラスを使用して環境内のストレージを標準化および管理するプロセスについて説明します。

1. ストレージクラスポリシーの作成 - ポリシーは、ストレージ動作の個々の側面（パフォーマンス目標、容量設定、セキュリティ要件、データ保護スケジュール）を定義します。ストレージクラスを構築する前に、ポリシーを作成してください。
2. ストレージクラスの作成 - 該当する各カテゴリから1つのポリシーを組み合わせてストレージクラスを作成します。事前定義されたストレージクラスを使用するか、組織の基準に合わせてカスタムのストレージクラスを作成することができます。

3. ストレージクラスをフリートに関連付ける - ストレージクラスを作成したら、プロビジョニングとコンプライアンス監視に使用するフリートに関連付けます。
4. ストレージクラスを使用してストレージをプロビジョニングする - ボリュームまたは LUN をプロビジョニングする際に、個々の設定を構成する代わりにストレージクラスを選択します。Console のローカル展開では、クラスを使用して最適なクラスタ配置を推奨し、クラスで定義された設定でプロビジョニングを行います。
5. ワークロードのずれを監視する - Console のローカル展開では、各ワークロードをストレージクラスにエンコードされた標準と照らし合わせて継続的に評価します。設定のずれやパフォーマンスの不適合が発生した場合、その問題にフラグが付けられ、アラートが発生する可能性があります。
6. ドリフトを修復してコンプライアンスを回復する - ドリフトまたはパフォーマンスの非コンプライアンスが検出された場合、ガイド付き手順に従って問題を手動で修正したり、Console のローカル展開で一般的なドリフト状態を自動的に解決したり、設定を変更する必要がある場合はワークロードをストレージ クラスから切り離したりできます。

ストレージクラスがフリートとどのように連携するか

ストレージクラスはフリートに関連付けられています。ストレージクラスをフリートに関連付けると、そのクラスはフリート内のすべてのプロビジョニングで使用できるようになります。これにより、フリート内でプロビジョニングされるすべてのワークロードが同じ標準に従うことが保証され、フリートは関連するクラスター全体で一貫したストレージ動作を適用するための主要な手段となります。

フリートの整理方法の詳細については、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。

次のステップ

- フリート編成を理解するには、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。
- ポリシーとストレージ クラスを作成するには、"ストレージクラスとポリシーを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"
- "AI支援によるストレージの提供"
- ドリフトの分析と修正については、"ストレージクラスのずれを修正する"を参照してください。

NetApp Console ローカル展開における LLM 統合について

NetApp Console のローカル展開は、AI支援によるストレージ管理のために、大規模言語モデル（LLM）に接続します。セットアップ後、ユーザーは自然言語を使用してストレージをプロビジョニングしたり、アラートを調査したり、ストレージに関するガイダンスを取得したりできます。

LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

AI支援による管理機能により、ユーザーは平易な言葉でリクエストを記述でき、Console のローカル展開でお

客様のストレージポリシーが適用されます。

コンソールローカル展開では、LLMリクエストは設定したエンドポイントにのみ送信されます。

AIを活用したストレージ管理でできること

LLM統合を有効にすると、Console ローカル展開はConsole アシスタントを通じて次の3つの機能を提供します。

- ストレージプロビジョニング ワークロード要件を平易な言葉で説明してください。Console のローカル展開機能は、ストレージクラスに基づいてプロビジョニングプランを推奨し、実行します。
- アラートへの対応 Console のローカルデプロイメントにアクティブなアラートの調査を依頼します。問題を分析し、割り当てられた権限に基づいてアクションを提案または実行します。
- 検索とガイダンス ストレージ環境またはONTAP管理について質問できます。NetApp Console のローカルデプロイメントは、ドキュメントと現在のフリートの状態から状況に応じた回答を返します。

Console アシスタントの読み取り専用または読み取り / 書き込みアクセスを選択する

ユーザーは、望む結果に基づいてアシスタントのアクセスモードを選択します：

- インフラストラクチャの変更を行わずにガイダンスや調査を行うための*読み取り専用*モード。
- ガイド付き実行のための*読み取り / 書き込み*モード。コンソールのローカルデプロイメントでは、提案されたアクションが表示され、確認を求めた後、変更が実行されます。

コンソールアシスタントのアクションを制御するものを理解する

コンソールのローカル展開は、プラットフォーム全体で使用されているのと同じガバナンスモデルを通じて、コンソールアシスタントのアクションを制御します：

- 役割ベースのアクセス制御は、各ユーザーが見たり実行したりできる内容を制限します。
- ストレージポリシーは、プロビジョニングおよび関連するアクションを制約します。
- コンソールアシスタントは、ストレージを変更する操作を実行する前に確認を求めます。

LLMプロバイダーパスを選択する

NetApp Console のローカル展開では、以下の LLM プロバイダータイプがサポートされます：

- **OpenAI**：OpenAIモデルへの直接アクセス。
- エンタープライズゲートウェイやプロキシサービスなどの互換性のあるエンドポイントに対応した **OpenAI-compatible** 。
- Anthropic の Claude モデル用。

モデルの可用性は、設定するエンドポイントによって異なります。Console のローカルデプロイメントで、リストからモデルを選択してください。

サポートされているモデルの詳細については、"NetApp Console ローカル展開でサポートされている LLM プロバイダーとモデルについて説明します"を参照してください。

LLMリクエストの送信先を理解する

データの流れは、選択したエンドポイントパスによって異なります。

- OpenAIエンドポイントを設定すると、コンソールのローカルデプロイメントはプロンプトとコンテキストをOpenAIエンドポイントに送信します。
- OpenAI互換エンドポイントを設定すると、Console のローカルデプロイメントは、組織が設定した互換エンドポイントにプロンプトとコンテキストを送信します。

LLM認証情報を保護し、管理者アクセスを制御する

これらの制御機能を使用して統合を保護します：

- APIキーは特権認証情報として扱い、組織のポリシーに従って定期的に更新してください。
- プロバイダー側の使用状況とアラートを確認し、予期しないアクティビティを検出します。

LLMを接続する

これらの決定を下したら、"LLMを接続してNetApp Consoleアシスタントを有効にする"に進みます。

接続または実行時チェックが失敗した場合は、"LLM統合のトラブルシューティング"を参照してください。

NetApp Console ローカル展開における NetApp Backup and Recovery について

NetApp Backup and Recovery は、ボリューム、データベース、仮想マシン、Kubernetes ワークロードなど、すべての ONTAP ワークロードに対して効率的で安全かつ対費用効果の高いデータ保護を提供するデータサービスです。

ワークロードとは、システム内のリソースを論理的にグループ化したものであり、保護、ガバナンス、検出、および復旧のために単一の単位として管理されます。Backup and Recoveryにおいて、ワークロードとは保護対象となる単位のことです。その意味はデータソースによって異なります：Kubernetesの場合、ワークロードはアプリケーションであり、VM環境の場合は仮想マシンであり、データベース環境の場合はデータベースです。

バックアップとリカバリのサポートは、すべての ONTAP システムにすでに組み込まれているため、追加のハードウェアやメディアゲートウェイは不要です。これにより、バックアップ作業がシンプルになり、コスト効率も向上します。NetApp Console を使用すると、複数のリソースマネージャや専門の担当者を必要とせずに、3-2-1 バックアップのすべてのバリエーションを含む、あらゆるバックアップ戦略の実装を簡素化できます。

NetApp Backup and Recovery は NetApp Console ローカル展開のプレビューモードです。本サービスはまだ一般提供されておらず、機能は変更される可能性があります。

"NetApp Backup and Recovery の詳細をご確認ください。".

インストールとセットアップ

NetApp Console ローカル展開のセットアップのクイックスタート

NetApp Consoleのローカル デプロイをインストールした後、適切なチームが適切なストレージ リソースを安全に管理できるように組織をセットアップします。このチェックリストを使用して、構造の計画、リソースの整理、メンバーの追加、統合の構成、およびデータ サービスの有効化を行ってください。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

1 NetApp Console ローカル展開のインストール

- インストールワークフローを確認して、導入プロセスを理解してください。"NetApp Console ローカル展開のインストールワークフローについて"。
- お客様のvCenterにNetApp Consoleのローカル展開をインストールします。"NetApp Consoleのローカル展開のインストール"。

2 組織を計画する

- フォルダとフリートを使ってリソースを整理する方法を学びましょう。"フォルダーとフリートについて"。
- ロールベースアクセス制御（RBAC）がメンバーに必要なアクセス権限を付与する仕組みを説明します。"NetApp Console ローカル展開におけるロールベースアクセス制御について学ぶ"。
- アイデンティティとアクセス管理ワークフローを確認します。"フリートおよびリソース管理のためのIAMを始める"。

3 組織を設定する

- ストレージシステムを NetApp Console ローカル展開に追加します。"ストレージ システムの追加"。
- 自社の事業構造に合ったフォルダとフリートの階層構造を作成してください。"フォルダとフリートを作成する"。
- リソースを適切なフォルダーとフリートに関連付けます。"リソースをフォルダーとフリートに関連付ける"。
- メンバーを追加し、初期の役割を割り当てます。"メンバーを追加して役割を割り当てる"。

4 統合とサービスの設定

- Active Directoryと統合することで、ディレクトリユーザーがコンソールのローカル展開にアクセスできるようにします。"Active Directoryとの統合"。
- 大規模言語モデル（LLM）を接続することで、コンソールアシスタントとAI支援による管理が可能になります。"LLMを接続する"。
- コンソールのローカル展開における通知配信方法を設定します。"通知配信の設定"。

5 **NetApp Backup and Recovery**のセットアップ

- "NetApp Backup and Recovery のライセンスを取得する"。高度なバックアップおよびリカバリサービスへのアクセスが不要な場合は、この手順をスキップできます。
- NetApp Console ローカル展開に NetApp Backup and Recovery ライセンスを追加します。"NetApp Consoleのローカル デプロイにライセンスを追加します"。
- "ユーザーに NetApp Backup and Recovery へのアクセス権を付与する".

NetApp Consoleのインストール

vCenterでOVAを使用してNetApp Consoleのローカルデプロイをインストールします

OVAを使用して、vCenterにNetApp Consoleのローカルデプロイメントをインストールします。OVAのダウンロードまたはURLは、NetApp Support Siteから入手できます。

NetApp Consoleのローカル デプロイのインストール準備

インストール前に、VM ホストが要件を満たしていること、および NetApp Console のローカル展開がインターネットおよび対象ネットワークにアクセスできることを確認してください。NetApp Backup and Recovery などの NetApp データサービスを使用するには、NetApp Console のローカル展開がお客様に代わって操作を実行できるよう、クラウド プロバイダの認証情報を作成してください。

NetApp Console ローカル展開ホスト要件の確認

NetApp Console ローカル展開をインストールする前に、ホストマシンがインストール要件を満たしていることを確認してください。

- CPU：16コアまたは16 vCPU
- RAM：64 GB
- ディスク容量：596 GB（シックプロビジョニングを推奨）
- vSphere 7.0u3以降、仮想ハードウェアバージョン19以降

NetApp Console のローカル展開は、ESXi ホスト上に直接インストールするのではなく、vCenter 環境にインストールしてください。

NetApp Console ローカル展開のネットワーク アクセスを設定する

NetApp Consoleのローカル展開では、サービス間通信に固定アドレス空間が使用されます。内部ネットワークには、IPアドレス範囲10.42.0.0/16と10.43.0.0/16が使用されます。Console のローカル展開を展開する前に、これらのIPアドレス範囲が、Console のローカル展開で使用可能なVLAN上の他のVM、DHCPスコープ、DNSレコード、またはロードバランサーのVIPプールに割り当てられていないことを確認してください。

エージェントのインターフェースのIPアドレスを変更する方法については、ナレッジベースの記事「Agent IP conflict with existing network」を参照してください。

VCenter環境に**NetApp Console**ローカルデプロイメントをインストールする

NetApp は、NetApp Console のローカル デプロイメントを vCenter 環境にインストールすることをサポートしています。OVA ファイルには、VMware 環境にデプロイできる事前設定済みの VM イメージが含まれています。

OVAをダウンロードするか、**URL**をコピーします。

OVAをダウンロードします。

1. NetApp Support Site から Console ローカル展開ソフトウェアをダウンロードしてください。

VCenter に **NetApp Console** のローカル展開を行います。

コンソールのローカル デプロイメントを展開するには、VCenter 環境にログインしてください。

手順

1. 環境によっては、自己署名証明書を信頼済み証明書にアップロードする必要があります。インストール後、この証明書を置き換えることができます。
2. コンテンツライブラリまたはローカルシステムからOVAを展開します。

ローカルシステムから	コンテンツライブラリより
a. 右クリックして「OVF テンプレートの展開…」を選択します。 b. URL から OVA ファイルを選択するか、ファイルの場所を参照して選択し、「次へ」を選択します。	a. コンテンツライブラリに移動し、コンソール OVA を選択します。 b. 「アクション」 > 「このテンプレートから新しい VM を作成」を選択します。

3. Console をデプロイするには、OVF テンプレートのデプロイ ウィザードを完了してください。
4. VMの名前とフォルダを選択し、*次へ*を選択します。
5. コンピューティング リソースを選択し、*次へ*を選択します。
6. テンプレートの詳細を確認し、*次へ*を選択します。
7. ライセンス契約に同意し、*次へ*を選択します。
8. 使用するプロキシ設定の種類を選択してください：明示的プロキシ、透過的プロキシ、またはプロキシなし。
9. VMをデプロイするデータストアを選択し、*Next*を選択します。ホストの要件を満たしていることを確認してください。
10. VMを接続するネットワークを選択し、*次へ*を選択します。ネットワークがIPv4であり、必要なエンドポイントへのアウトバウンドインターネットアクセスがあることを確認します。
11. 「テンプレートのカスタマイズ」ウィンドウで、以下の項目を入力してください：
    - プロキシ サーバ情報
      - 明示的なプロキシを選択した場合は、プロキシ サーバのホスト名またはIPアドレスとポート番号、およびユーザー名とパスワードを入力してください。
      - 透過型プロキシを選択した場合は、該当する証明書をアップロードしてください。
    - 仮想マシンの構成

- 設定チェックをスキップ：このチェックボックスはデフォルトではオフになっています。つまり、NetApp Console のローカル展開では、ネットワーク アクセスを検証するための構成チェックが実行されます。
  - NetApp では、このボックスのチェックを外したままにしておくことをお勧めします。そうすることで、インストール時に NetApp Console ローカル展開の構成チェックが実行されます。構成チェックは、NetApp Console のローカル展開が必要なエンドポイントへのネットワーク アクセスを持っているかどうかを検証します。接続の問題によりデプロイが失敗した場合は、NetApp Console ローカル展開ホストから検証レポートとログにアクセスできます。場合によっては、NetApp Console のローカル展開がネットワーク アクセスを持っていることが確実であれば、チェックをスキップすることもできます。
- メンテナンスパスワード： `maint`ユーザーのパスワードを設定します。このユーザーは NetApp Console ローカルデプロイメントメンテナンスコンソールへのアクセスを許可されています。
- **NTP** サーバ：時刻同期に使用する NTP サーバを 1 つ以上指定します。
- ホスト名：この仮想マシンのホスト名を設定します。検索ドメインを含めないでください。たとえば、FQDN が console10.searchdomain.company.com の場合は、console10 と入力してください。
- プライマリ**DNS**：名前解決に使用するプライマリ DNS サーバを指定します。
- セカンダリ **DNS**：名前解決に使用するセカンダリ DNS サーバを指定します。
- 検索ドメイン：ホスト名を解決する際に使用する検索ドメイン名を指定します。例えば、FQDN が console10.searchdomain.company.com の場合、searchdomain.company.com と入力します。
- **IPv4**アドレス：ホスト名にマッピングされるIPアドレス。
- **IPv4**サブネットマスク：IPv4アドレスのサブネットマスク。
- **IPv4**ゲートウェイアドレス：IPv4アドレスのゲートウェイアドレス。

12. 「次へ」を選択します。
13. 「完了の準備」ウィンドウで詳細を確認し、「完了」を選択します。

    vSphere タスクバーには、NetApp Console のローカル展開が配備される際の進行状況が表示されます。

14. VMの電源をオンにします。

コンソールの整理方法を計画する

NetApp Console ローカル展開での**ID**とアクセス管理の開始

NetApp Console のローカル展開では、フォルダとフリートの階層を設定し、メンバーと初期権限を追加し、適切なチームがアクセスして管理できるように、リソースを適切なフリートに追加して配置します。

必要なアクセスロール

スーパー管理者、組織管理者、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"。

初期設定を完了するには、**Organization admin** または **Super admin** のロールが必要です。セットアップ後は、組織の変更に応じて、リソース、メンバーアクセス、およびフリートアクセスを管理します。

1 リソースの追加または検出

Console のローカル展開にシステムを追加します。初期設定時には、通常、デフォルトのフリートが選択されている状態でシステムが追加されます。

リソースの作成方法や検出方法について説明します。

- "オンプレミス ONTAP クラスター"

2 フォルダとフリート階層を作成する

自社の組織構造に合わせて、追加のフリートとフォルダを作成します。

"フォルダとフリートを使ってリソースを整理する方法を説明します。".

3 リソースを適切なフリートに関連付ける

コンソールのローカルデプロイメントでシステムを追加または検出すると、そのリソースは現在選択されているフリートに自動的に関連付けられます。システムを適切なチームが利用できるようにするには、組織階層内の適切なフリートにシステムを関連付けます。

- "フォルダとフリート内のリソースを管理する方法について説明します。".

4 メンバーを追加し、開始時の権限を割り当てる

メンバーを追加し、管理対象に基づいて、組織、フォルダ、またはフリートレベルで役割を割り当てます。

"メンバーとその権限を管理する方法を説明します".

初期設定後

初期設定が完了したら、組織の変更に合わせてアクセス権限とリソースの配置を管理します。

- "フォルダーとフリートでリソースを管理する"
- "フリートやフォルダ全体にわたるメンバーアクセス管理（メンバー中心）"
- "特定のフリートまたはフォルダへのアクセス権限を管理する（フリート中心）"
- "不要になったフォルダとフリートを削除する"

関連情報

- "NetApp Console のアイデンティティとアクセス管理について"
- "IDとアクセス管理のAPIについて"

NetApp Console ローカル展開におけるフォルダーとフリートについて

NetApp Console のローカル展開では、フォルダーとストレージフリートを使用して、場所、部門、またはワークロードタイプ別に、ビジネス構造に応じた NetApp リソースの

整理とアクセス制御を行います。

このページは、階層構造戦略とフリート設計パターンに関する情報を提供しています。メンバー、ロール、リソーススコープの完全な IAM モデルについては、"NetApp Console ローカル展開におけるアイデンティティとアクセス管理について"。

リソースは階層構造で整理されます。最上位に組織があり、その下にフォルダ（他のフォルダやフリートを含むことができる）、そしてストレージシステムを含むフリートが続きます。組織、フォルダ、またはフリートレベルでアクセスロールを割り当てることで、ユーザーがリソースに適切なアクセス権限を持つようにします。

NetApp Console のローカル展開でフォルダーとフリートを管理するには、組織管理者、フォルダーまたはフリート管理者の役割が必要です。

組織構成要素

組織構成要素（組織、フォルダ、フリート）は階層構造を形成し、リソースのグループ化方法とアクセス権の委任方法を決定します。

組織

組織はNetApp Consoleのローカル展開階層の最上位であり、通常はお客様の会社を表します。組織は、フォルダ、フリート、メンバー、役割、およびリソースで構成されています。リソースはフリートに関連付けられ、メンバーには組織、フォルダ、またはフリートレベルで役割が割り当てられます。

フォルダ

フォルダは、関連するフリートをグループ化し、場所、拠点、または事業部門ごとに整理します。ストレージシステムをフォルダに直接関連付けることはできませんが、フォルダレベルでメンバーにロールを割り当てると、そのフォルダ内のすべてのフリートへのアクセス権が付与されます。

組織管理者は、リソースをフォルダーに追加することで、そのリソースをフリートに関連付けるタスクをフォルダー管理者またはフリート管理者に委任できます。"リソースをフォルダーとフリートに関連付ける"。

フリート

フリートはストレージシステムをグループ化します。フリートにリソースを割り当て、フリートレベルでメンバーにアクセス権を付与します。リソースは複数のフリートに属することができます。フリートへのアクセス権を持つメンバーは、そのフリート内のリソースを管理できます。

例えば、ニーズに応じて、オンプレミスの ONTAP システムを単一のフリートまたは組織内のすべてのフリートに関連付けることができます。

"フォルダとストレージフリートの作成方法を説明します".

リソース

リソースとは、コンソールのローカル展開が認識し、フリートに割り当てることができるストレージシステムのことです。リソースをフリートに関連付けることで、フリートへのアクセス権を持つユーザーがリソースを管理できるようになります。

例えば、ONTAP クラスタを組織内の1つのフリート、またはすべてのフリートに関連付けることができます。リソースをどのように関連付けるかは、組織のニーズによって異なります。

"リソースをフリートに関連付ける方法を説明します".

メンバーと役割

メンバーとは、組織内のユーザーおよびサービスアカウントのことです。役割は、組織、フォルダ、フリートといった階層構造のどのレベルで、どのようなアクションを実行できるかを定義します。

Members

組織のメンバーは、ユーザーアカウントまたはサービスアカウントのいずれかです。サービスアカウントは通常、アプリケーションが人間の介入なしに特定のタスクを完了するために使用されます。

組織管理者権限を持つユーザーは、組織に新しいメンバーを追加できます。コンソールのローカル展開にアクセスするには、すべてのユーザー（サービスアカウントおよびActive Directoryユーザーを含む）を明示的に追加し、少なくとも1つのロールを付与する必要があります。

"組織にメンバーを追加する方法を説明します".

アクセスロール

コンソールのローカル展開では、組織のメンバーに割り当てることができるアクセスロールが提供されます。

メンバーにロールを関連付けると、そのロールを組織全体、特定のフォルダ、または特定のフリートに付与できます。選択したロールによって、メンバーは階層構造の選択した部分にあるリソースへのアクセス権限を得ます。

NetApp Console のローカル展開では、最小権限の原則に準拠したきめ細かなロールが提供されます。つまり、アクセスロールは、メンバーが必要とするものにのみアクセスできるように設計されています。

ユーザーは、職務範囲の拡大に伴い、複数の役割を担うことができます。

役割継承

組織レベルまたはフォルダレベルでロールを割り当てると、その下の子フォルダ、フリート、およびリソースはそのロールを継承するため、フォルダとフリートの設計によって、各割り当ての適用範囲が決まります。

"NetApp Console ローカル展開におけるロール継承について".

組織設計の例

適切な組織構造は、組織の規模とチームの編成方法によって異なります。以下の例は、さまざまな組織がフォルダとフリートの階層構造を利用してアクセスを効果的に管理する方法を示しています。

小規模組織戦略

ユーザー数が50人未満で、ストレージ管理が一元化されている組織の場合は、Super admin と Super viewer のロールを使用した簡略化されたアプローチを検討してください。

例：**ABC Corporation**（**5**人チーム）

- 構造：3つのフリート（本番環境、開発環境、バックアップ環境）を持つ単一組織
- 役割：

- 上級メンバー2名：完全な管理アクセス権限を持つスーパー管理者ロール
- チームメンバー3名：変更権限なしで監視するためのスーパービューアーロール

- メリット：管理の簡素化、役割の複雑さの軽減、幅広いアクセス権限を必要とするチームに適しています

多地域展開企業戦略

地域ごとの事業展開や専門チームを持つ大規模組織の場合は、地理的境界や事業部門の境界を表すフォルダを用いた階層的なアプローチを採用してください。

例：**XYZ Corporation**（多国籍企業）

- 構造：組織 > 地域フォルダ（北米、ヨーロッパ、アジア太平洋） > 地域別フリート
- プラットフォームの役割：
  - 1 組織管理者：グローバルな監督とポリシー管理
  - 3 フォルダーまたはフリート管理者：地域制御（地域ごとに1人）
  - 1 フェデレーション管理者：企業ディレクトリサービスの統合
- 地域別のストレージロール：
  - ストレージ管理者：割り当てられたリージョン内のストレージシステムを検出および管理します
  - ストレージビューア：リージョンをまたいでストレージリソースを監視する
  - システムヘルススペシャリスト：システム変更なしでストレージの状態を管理
- メリット：役割分担、地域ごとの自治、および現地規制の遵守によるセキュリティの強化

部門専門化戦略

特定のアクセス権限を必要とする専門チームを持つ組織では、職務上の責任に基づいた、対象を絞った役割割り当てを使用してください。

例：**TechCorp**（中規模テクノロジー企業）

- 構造：組織 > 部門フォルダ（IT、セキュリティ、開発） > フリート固有のリソース
- 専門的な役割：
  - セキュリティチーム：ランサムウェア耐性管理者および分類ビューアーの役割
  - バックアップチーム：包括的なバックアップ操作を行うバックアップおよびリカバリのスーパー管理者
  - 開発チーム：ストレージ管理者（テスト環境管理）
  - コンプライアンスチーム：監視およびサポートケース管理のための運用サポートアナリスト
- メリット：カスタマイズされたアクセス制御、運用効率の向上、専門業務に対する明確な責任体制

次の手順

- "フォルダとストレージフリートを作成する"
- "リソースをフォルダーとフリートに関連付ける"

- "フリートアクセス割り当ての管理"
- "コンソールのローカル展開アクションを監視または監査する"

NetApp Console ローカル展開におけるロールベースアクセス制御について学ぶ

ロールベースアクセス制御（RBAC）を使用して、NetApp Console ローカルデプロイメントへのユーザーアクセスを管理します。組織、フォルダ、またはフリートレベルで事前定義されたロールを割り当てることができます。各ロールには、ユーザーが割り当てられたスコープ内で実行できる操作を定義する特定の権限が付与されます。

NetApp Console のローカル展開ロールは、最小権限の原則に基づいて設計されているため、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。このアプローチは、各メンバーが必要とするアクセスを制限することで、セキュリティを強化します。

リソースをフォルダーやフリートに整理したら、組織のメンバーに特定のフォルダーやフリートに対する役割を割り当て、各メンバーがそれぞれの責任のみを果たすようにします。

例えば、特定のフリートレベルに対してバックアップおよびリカバリの管理者ロールをメンバーに割り当てることで、そのメンバーは組織全体への広範なアクセス権を付与されることなく、そのフリート内のリソースに対するバックアップおよびリカバリ操作を実行できるようになります。この同一ユーザーには、組織内の複数のフリートに対するロールを付与することができます。

メンバーには、責任範囲に応じて、同じスコープまたは異なるスコープで複数のロールを割り当てることができます。例えば、小規模な組織では、組織レベルで Storage admin と Backup and Recovery admin の両方のロールを同じメンバーに割り当てる場合がある一方、大規模な組織では、フリートレベルでそれぞれのロールに異なるメンバーを割り当てる場合があります。

コンソール組織メンバーの種類

NetApp Console のローカル展開では、以下の種類のメンバーがサポートされます：

- ユーザー: 個々のユーザーは、ローカル認証情報を使用する NetApp Console ローカルデプロイメントに追加するローカルユーザー、または統合された Active Directory または LDAP サービスを介して認証を行うディレクトリユーザーのいずれかです。どちらのタイプのユーザーにも、リソースにアクセスするための NetApp Console ローカルデプロイメントでロールを割り当てることができます。
- サービスアカウント：アプリケーションやサービスが API を介して NetApp Console のローカル展開と連携するために使用する非人間アカウント。サービスアカウントをコンソールのローカル展開組織に直接追加できます。

"組織にメンバーを追加する方法を説明します。"

NetApp Console ローカル展開における事前定義済みロール

NetApp Console のローカル展開には、組織メンバーに割り当てることができる事前定義済みのロールが含まれています。各ロールには、メンバーが割り当てられたスコープ（組織、フォルダ、またはフリート）内で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 のローカル展開ロールは、最小権限の原則を使用して、メンバーがタスクに必要な権限のみを持つことを保証し、提供するアクセスの種類ごとにロールを分類します：

- プラットフォームロール：コンソールのローカルデプロイメント管理権限を提供する

- 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、Console のローカルデプロイメントイベントおよびアラートの監査に関する権限を提供します。

メンバーの責任に基づいて、複数のロールを割り当てることができます。例えば、特定のフリートに対して、Storage admin ロールと Backup and Recovery admin ロールの両方をメンバーに割り当てることができます。

メンバーのアクセス権限を選択するには、役割カテゴリをメンバーの責任範囲に合わせ、次に、メンバーがどの程度のアクセス権限を持つべきかに応じて、スコープ（組織、フォルダ、またはフリート）で役割を割り当てます。"さまざまな組織がNetApp Consoleのローカル展開において、どのようにロールとスコープを構成しているかについて説明します。"。

"NetApp Console ローカル展開でメンバーに割り当てることができる事前定義済みロールについて説明します".

役割継承の仕組み

組織レベルまたはフォルダレベルでロールを割り当てると、そのロールは階層構造のその部分内の子スコープに継承されます。これは、組織レベルのロールは組織全体に適用され、フォルダレベルのロールはそのフォルダ内のすべての子フォルダとフリートに適用され、フリートレベルのロールはそのフリート内のリソースにのみ適用されることを意味します。

メンバーに保持させたいアクセス権限に一致するスコープを使用してください。例えば、メンバーが同一地域内の複数のフリートに対して同じアクセス権限を必要とする場合、フォルダレベルでロールを割り当てます。メンバーが1つのフリートのみにアクセスする必要がある場合は、フリートレベルでロールを割り当ててください。

下位スコープで継承されたアクセス権を上書きすることはできません。メンバーが組織またはフォルダーからロールを継承した場合、最初に付与した上位スコープでその割り当てを変更してください。

"NetApp Console ローカル展開におけるフォルダーとフリートについて"."メンバーアクセスを管理する"."フリートアクセス割り当ての管理".

Console の組織を設定する

フォルダーとフリートを**NetApp Console**のローカル展開組織に追加する

ビジネス構造に合わせてフォルダーとフリートを作成し、アクセスを制御し、NetApp Console ローカル展開でリソースを整理します。

必要なアクセスロール

スーパー管理者、組織管理者、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"。

NetApp Consoleのローカル展開では、組織を作成する際にデフォルトのフリートが1つ作成されます。フリートを追加して、フォルダでグループ化することができます。"NetApp Consoleのリソース階層について学ぶ"。

フォルダーとフリートを使用してリソースを整理する

フォルダーとフリートは、組織の構造をチームの実際の働き方に合わせて構築するために使用する2つの構成

要素です。例えば、地域ごとに1つのフォルダを作成し、それぞれのフォルダ内に本番環境用と開発環境用のフリートを配置するといった具合です。

- フォルダは関連するフリートをグループ化し、委任された管理とロールの継承をサポートします。
- フリートとは、管理のためにリソースを関連付け、ユーザーに運用アクセス権を付与する方法です。

先にフォルダやフリートを作成し、後からリソースやメンバーのアクセス権を追加することができます。これにより、Console のローカルデプロイメントでユーザーやリソースを追加する前に、リソース階層を計画することができます。構造が既に定義されている場合は、フリートを作成する際にリソースを追加し、アクセス権を割り当てることができます。フリートはいつでも更新できます。

例えば、本番環境用のクラスターを本番環境用のフリートに、テスト環境用のクラスターをテスト環境用のフリートに配置し、各チームには自チームが所有するフリートへのアクセス権のみを付与します。

フォルダ

フォルダを使用すると、ビジネスユニット、地域、チームなどのビジネス構造ごとにフリートを整理できます。フォルダをネストして、組織を反映させることができます。

フォルダレベルで割り当てられた役割は、子フォルダおよびフリートに継承されます。フォルダを使用すると、階層構造のその部分を担当するフォルダ管理者またはフリート管理者に、フリート割り当てタスクを委任することもできます。

> メンバーはフォルダ単位ではなく、フリート単位で作業を行います。フォルダのみに関連付けられたリソースは、フリートに関連付けられるまでメンバーによって管理できません。

例えば、地域企業はフォルダーを使用して、事業部門別およびワークロード別に ONTAP ストレージを整理できます。北米用のトップレベルフォルダー、本番環境および開発環境用のサブフォルダー、SAP、VMware、およびバックアップボリュームをホストする ONTAP クラスター用のフリートを作成することができます。北米フォルダーに割り当てられたストレージ管理者は、すべての子フリートへのアクセス権を継承しますが、アプリケーションチームは、自身が管理するフリートへのアクセス権のみを持ちます。

フリート

メンバーが管理できるように、リソースをフリートに関連付けます。フリートは、組織の直下またはフォルダ内に存在できます。

例えば、ある医療会社は、本番環境と開発環境の別々のフリートでONTAPストレージを使用しています。本番フリートはクリニカルアプリと電子カルテデータベースを実行し、開発フリートはテストと検証をサポートします。この分離により、ライブデータが保護され、本番環境へのアクセスがより厳格に管理され、監査可能性と最小権限の原則が確保されるとともに、開発チームは患者向けワークロードに影響を与えることなく作業を進めることができます。

ユーザーは「システム」ページで割り当てられたフリート間を移動し、各フリートに関連付けられたリソースを管理します。

フォルダーまたはフリートを追加する

リソースやメンバーのアクセスに関する新たな境界が必要な場合はいつでもフリートを追加し、関連するフリートをグループ化して管理を委任したい場合はフォルダを追加してください。例えば、 `Production`フォルダーに `Production-US-East`フリートと `Production-EU-West`フリートを追加し、そのフリートのみに対して、地域リーダーにフォルダーまたはフリート管理者ロールを割り当てます。

最大7階層まで作成できます。

フリートやフォルダを作成する際にリソースを追加したり、メンバーのアクセス権を割り当てたりすることができます。後から行うことも可能です。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. **Organization** を選択します。
3. 「組織」ページから、「フォルダーまたはフリートの追加」を選択します。
4. 「フォルダー」または「フリート」を選択してください。
5. 名前と場所：フォルダまたはフリートの名前を入力し、場所を選択します。

1. オプション：*リソース*セクションを展開して、リソースをフリートまたはフォルダに関連付けます。
   a. 関連付けたいリソースの横にあるチェックボックスをオンにしてから、*フリートに関連付ける*を選択してください。Console のローカル展開にシステムをまだ追加していない場合は、この手順は後で行うことができます。

   メンバーは、フォルダ内のリソースがフリートに割り当てられるまで、そのリソースにアクセスできません。

2. オプション：*アクセス*セクションを展開して、メンバーにアクセス権限を割り当てます。*メンバーを追加*を選択して、アクセス権と役割を割り当てます。デフォルトでは、フリートを作成したユーザーがそのフリートにアクセスできます。

   "アクセスロールについて".

3. *追加*を選択します。

フォルダまたはフリートの名前を変更する

必要に応じて、フォルダまたはフリートの名前を変更します。名前変更は、関連するリソースやメンバーのアクセス権には影響しません。

手順

1. 「組織」ページから、テーブル内のフリートまたはフォルダーに移動し、•••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. 「編集」ページで、新しい名前を入力し、「適用」を選択します。

フォルダまたはフリートを削除する

チームの再編成後やフリートの完了後など、不要になったフォルダやフリートを削除します。

フォルダまたはフリートを削除する前に、以下のチェックを完了してください：

- フォルダまたはフリートにリソースが含まれていないことを確認してください。"リソースの関連付けを削除する方法を説明します"。
- フォルダまたはフリートへのアクセス権をまだ持っているメンバーを確認してください。"メンバーのアクセス権限の割り当てを表示する"。

- 必要に応じて、メンバーのアクセス権を削除または更新してください。"メンバーのアクセス権限の割り当てを変更する"。
- フリートを削除する場合は、まずリソースをターゲットフリートに移動してください。"フリート間でリソースを移動する方法を説明します"。

手順

1. 「組織」ページから、テーブル内のフリートまたはフォルダーに移動し、•••を選択してから「削除」を選択します。
2. フォルダまたはフリートを削除することを確認してください。

NetApp Console ローカル展開でフリートとフォルダーを管理する

初期設定後、以下の操作が可能です：

- フォルダとフリートのリソース関連付けを管理する："リソースをフリートやフォルダーに関連付ける方法について説明します。"
- 1つのフォルダーまたはフリートのアクセス権を表示または更新する："ユーザーにフリートへのアクセス権を付与する方法について説明します。"
- 複数のフォルダとフリートにわたって1人のメンバーを管理する："メンバーアクセスの管理方法について説明します"
- メンバーを追加し、開始時の権限を割り当てます："メンバーと権限の管理方法について説明します"。

関連情報

- "NetApp Console のアイデンティティとアクセスについて"
- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "フリートアクセス割り当ての管理"
- "IDおよびアクセスAPIについて"

ストレージシステムを NetApp Console ローカル展開に追加する

ストレージ システムを NetApp Console ローカル展開に追加することで、ストレージ インフラストラクチャの監視、インベントリ管理、および管理が可能になります。ストレージ システムが追加されると、Console ローカル展開によってシステムが検出され、監視および管理タスクに使用できる情報の収集が開始されます。

開始する前に、ストレージ システムを追加するために必要な権限があること、およびストレージ システムが Console のローカル展開からアクセス可能であることを確認してください。

手順

1. 「ストレージ」>「管理」を選択します。
2. 「スコープ」ドロップダウンリストから、ストレージ システムを追加するフリートを選択します。
3. 「システムを追加」を選択します。
4. 接続情報や認証情報など、必要なストレージシステムの詳細を入力してください。
5. 入力した情報を確認し、*追加*を選択します。

ストレージシステムが選択されたフリートに追加されます。Console のローカル展開により、システムの検出と監視が開始されます。環境やネットワーク接続状況によっては、システムが完全に管理対象として認識されるまでに数分かかる場合があります。

また、**[管理] > [IDとアクセス]** ページから **[システムの追加]** を選択し、必要なシステム情報を入力することで、ストレージ システムを追加することもできます。

フォルダーとフリート内のリソースを **NetApp Console** ローカル展開で管理する

リソースを適切なフォルダーまたはフリートに関連付けることで、NetApp Console のローカル展開におけるリソースアクセスを管理します。これにより、どのチームがリソースにアクセスして管理できるかを制御できます。

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"。

適切なチームが管理できる場所にリソースを配置し、所有権が変更された場合は移動させ、不要になった場合は関連付けを解除します。

リソースとは、Console のローカル展開で認識されるエンティティのことで、ストレージリソースやバックアップおよびリカバリワークロードなどが含まれます。

コンソールリソースタイプ

コンソールのローカル展開は、ストレージリソースとバックアップおよびリカバリワークロードの両方をサポートします。アクセスと管理を制御するために、いずれかのリソースタイプをフリートに関連付けます。

ストレージリソース

ストレージリソースは、組織内で最も一般的なリソースの種類です。Console のローカル展開にストレージシステムを追加する場合は、適切なチームがアクセスして管理できるように、フリートに関連付けてください。たとえば、ONTAP クラスターを追加した後、 `Production-US-East`フリートに関連付けてください。

バックアップおよびリカバリのワークロード

バックアップおよびリカバリのワークロードもリソースとみなされます。バックアップおよびリカバリワークロードをフリートに関連付けることで、メンバーにこれらのワークロードへのアクセス権限を割り当てることができます。例えば、メンバーがアクセスできるフリートにバックアップおよびリカバリワークロードを関連付け、適切なバックアップおよびリカバリロールを付与することで、そのメンバーにバックアップおよびリカバリワークロードへのアクセス権を割り当てることができます。

組織内のリソースを表示する

組織内のリソースを表示して、特定のリソースを見つけ、それがどのフリートまたはフォルダーに関連付けられているかを確認します。フォルダやフリートを作成していない場合、すべてのリソースは組織直下のデフォルトフリートに関連付けられます。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. 「リソース」を選択します。

3. 「高度な検索とフィルタリング」を選択します。
4. 利用可能なオプションを使用してリソースを検索します。
   - リソース名で検索：テキスト文字列を入力し、*追加*を選択します。
   - プラットフォーム：Amazon Web Servicesなど、1つ以上のプラットフォームを選択してください。
   - リソース：Cloud Volumes ONTAP など、1つ以上のリソースを選択してください。
   - 組織、フォルダ、またはフリート：組織全体、特定のフォルダ、または特定のフリートを選択します。
5. 「検索」を選択します。

リソースをフォルダーまたはフリートに関連付ける

適切なチームが管理できるように、リソースをフリートまたはフォルダに関連付けます。例えば、ONTAPクラスターを追加した後、 `Production-US-East`フリートに関連付けることで、そのフリートの地域ストレージ管理者が管理できるようになります。

組織管理者ロールを持つユーザーは、フォルダーにリソースを追加することで、そのフォルダーのフォルダー管理者またはフリート管理者にフリート関連付けタスクを委任できます。"リソースをフォルダーに関連付ける"。

手順

1. 「リソース」ページから、表内のリソースに移動し、 ••• を選択してから、「フォルダーまたはフリートに関連付ける」を選択します。
2. フォルダまたはフリートを選択し、次に*Accept*を選択します。
3. 追加のフォルダーまたはフリートを関連付けるには、*フォルダーまたはフリートの追加*を選択し、フォルダーまたはフリートを選択します。

   管理者権限を持つフォルダーとフリートのみを選択できます。

4. 「リソースを関連付ける」を選択します。
   - リソースをフリートに関連付けた場合、そのフリートに対する権限を持つメンバーは、Console からリソースにアクセスできるようになります。
   - リソースをフォルダーに関連付けた場合、_フォルダーまたはフリート管理者_は、そのリソースにアクセスして、フォルダー内のフリートに関連付けることができるようになります。"リソースをフォルダーに関連付ける"。

リソースに関連付けられているフォルダーとフリートを表示する

リソースがどのフリートまたはフォルダーに関連付けられているかを確認します。

リソースへのアクセス権を持つメンバーを確認するには、関連するフォルダーまたは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"。

手順

1. 「リソース」ページから、表内のリソースに移動し、 ••• を選択して、「詳細を表示」を選択します。

以下の例は、1つのフリートに関連付けられたリソースを示しています。

リソースへのアクセス権を持つメンバーを確認するには、関連するフォルダまたはフリートを確認してください。

"フリートアクセス割り当ての管理"."メンバーアクセスを管理する".

フォルダーまたはフリートからリソースを削除する

リソースとフォルダまたはフリートの関連付けを解除することで、メンバーがそこでリソースを管理できないようにします。

組織全体からストレージシステムを削除するには、**Systems** ページに移動してシステムを削除します。

手順

1. 「リソース」ページから、表内のリソースに移動し、•••を選択して、「詳細を表示」を選択します。
2. フォルダーまたはフリートからリソースを削除するには、フォルダーまたはフリートの横にある を選択します。
3. 関連付けを解除するには、*削除*を選択してください。

フリート間でリソースを移動する

リソースをあるフリートから別のフリートに移動するには、現在のフリートとの関連付けを解除してから、対象のフリートに関連付けます。

関連付けが変更されると、リソースへのアクセス権もすぐに変更されます。可能であれば、両方の手順を1回のメンテナンス時間内に完了してください。

手順

1. 「リソース」ページから、表内のリソースに移動し、•••を選択して、「詳細を表示」を選択します。
2. 現在のフリートの横にある を選択し、*削除*を選択します。
3. 「フォルダーまたはフリートを追加」を選択します。
4. 対象のフリートを選択し、**Accept** を選択します。
5. 「リソースを関連付ける」を選択します。

関連情報

- "NetApp Console のアイデンティティとアクセスについて"

- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "リソース移動後のフリートアクセス割り当てを管理する"
- "IDとアクセス管理のAPIについて"

メンバーを **NetApp Console** ローカル展開組織に追加する

メンバーを NetApp Console のローカル展開組織に追加し、ユーザー、サービスアカウント、ディレクトリユーザーに対して、組織、フォルダ、またはフリートレベルでのアクセス権を付与するロールを割り当てます。

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"。

開始する前に

- 組織に合ったフォルダとフリートの階層構造を作成してください。"フォルダとフリートを使ってリソースを整理する方法を説明します。"。
- メンバーのアクセス権を割り当てる前に、リソースを適切なフリートに関連付けてください。"フォルダとフリート内のリソースを管理する方法について説明します。"。
- ディレクトリユーザーを追加する場合は、まずディレクトリサービスを統合してください。"ディレクトリサービスとの統合方法をご確認ください"。

NetApp Console ローカル展開におけるアクセス許可の仕組みを理解する

NetApp Console はロールベースアクセス制御（RBAC）を使用して権限を管理します。必要なアクセス権限を付与するために、メンバーにロールを割り当ててください。各ロールは、特定のリソースに対して許可される操作を定義します。

NetApp Console ローカル展開でのアクセス許可に関する注意事項：

- ユーザーがリソースにアクセスするには、各ユーザーを組織に明示的に追加し、少なくとも1つのロールを割り当てる必要があります。
- 組織レベルまたはフォルダレベルで割り当てた役割は子スコープに継承されるため、メンバーが必要な場所でのみアクセスできるように、割り当てスコープを慎重に選択してください。"NetApp Console ローカル展開におけるロール継承について"。

組織にメンバーを追加する

NetApp Console は、ユーザーアカウント、ディレクトリユーザー、サービスアカウントの3種類のメンバーをサポートしています。

ユーザーを追加する前に、Console のローカル展開で使用するメールサーバーを最初に設定する必要があります。"メールサーバーの設定方法について説明します。"

ディレクトリユーザーは統合ディレクトリサービスを通じて認証されますが、Console のローカル展開では、各ディレクトリユーザーを個別に追加し、ロールを割り当てる必要があります。Console でサービスアカウントを直接作成します。

Console のローカル展開にアクセスするには、すべてのメンバーに少なくとも1つのロールが明示的に割り当てられている必要があります。

メンバーを追加する際は、メンバーがアクセスする必要のある組織、フォルダー、またはフリートを選択し、必要な初期ロールを割り当ててください。

ユーザーアカウントを追加する

組織、フォルダ、またはフリートにユーザーを追加してリソースにアクセスできるようにするには、組織管理者、フォルダ管理者、またはフリート管理者のいずれかの役割を持っ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. 「メンバーを追加」を選択します。
4. *メンバータイプ*については、*ユーザー*を選択したままにしてください。
5. 「ユーザーのメールアドレス」には、ユーザーが作成した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てください。
6. 「組織、フォルダ、またはフリートを選択」セクションを使用して、メンバーがアクセスする必要がある場所を選択します。

   次の点に注意してください。

   - 権限のあるフォルダーとフリートのみを選択できます。
   - 組織またはフォルダを選択すると、そのメンバーにそのすべてのコンテンツへのアクセス権限が付与されます。
   - 組織管理者ロールは、組織レベルでのみ割り当てることができます。
7. *カテゴリを選択*してから、選択した組織、フォルダー、またはフリートに対してメンバーに必要な初期権限を付与する*ロール*を選択してください。

   "アクセスロールについて".

8. より多くのフォルダー、フリート、またはロールへのアクセス権を付与するには、ロールの追加 を選択し、フォルダー、フリート、またはロールのカテゴリを選択して、ロールを選択します。
9. *追加*を選択します。

   コンソールはユーザーに指示をメールで送信します。

サービスアカウントを追加する

タスクを自動化したり、Console APIに安全に接続したりする必要がある場合は、サービスアカウントを追加してください。アカウントを作成したら、そのクライアントIDとクライアントシークレットをコピーして、使用する連携機能に渡してください。

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. 「メンバーを追加」を選択します。
4. 「メンバータイプ」には「サービスアカウント」を選択してください。
5. サービスアカウントの名前を入力してください。
6. 「組織、フォルダ、またはフリートを選択」セクションを使用して、サービスアカウントがアクセスする必要がある場所を選択します。

   次の点に注意してください。

   - 権限のあるフォルダーとフリートのみを選択できます。
   - 組織またはフォルダを選択すると、メンバーはその組織またはフォルダ内のすべてのコンテンツに対する権限が付与されます。
   - 組織管理者ロールは、組織レベルでのみ割り当てることができます。
7. 「カテゴリ」を選択し、次に、選択した組織、フォルダー、またはフリートに対してサービスアカウントに必要な初期権限を付与する「ロール」を選択します。

   "アクセスロールについて".
8. より多くのフォルダー、フリート、またはロールへのアクセス権を付与するには、ロールの追加 を選択し、フォルダー、フリート、またはロールのカテゴリを選択して、ロールを選択します。
9. 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。

   コンソールにはクライアントシークレットが一度だけ表示されます。安全な場所にコピーしておいてください。紛失しても後で再作成できます。
10. 「閉じる」を選択します。

組織にディレクトリユーザーを追加する

統合ディレクトリサービスからユーザーを追加し、最初のロールを付与します。例えば、Active Directory から新しいストレージエンジニアを追加し、 `Production-US-East`フリートでストレージ管理者ロールを割り当てることで、そのフリートで作業できるようにします。

ディレクトリユーザーを追加するには、まずディレクトリサービスを設定する必要があります。"ディレクトリサービスとの統合方法をご確認ください"。

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. 「メンバーを追加」を選択します。
4. 「メンバータイプ」には「ディレクトリユーザー」を選択してください。
5. 「ユーザーのメールアドレス」には、追加したいディレクトリユーザーのメールアドレスを入力してください。このメールアドレスは、ディレクトリ内でユーザーのログインに関連付けられているメールアドレスと一致している必要があります。
6. 「組織、フォルダ、またはフリートを選択」セクションを使用して、ディレクトリユーザーがアクセスする必要がある場所を選択します。

次の点に注意してください。

- 権限のあるフォルダーとフリートのみを選択できます。
- 組織またはフォルダを選択すると、メンバーはその組織またはフォルダ内のすべてのコンテンツに対する権限が付与されます。
- 組織管理者ロールは、組織レベルでのみ割り当てることができます。

7. *カテゴリ*を選択し、次に*役割*を選択して、選択した組織、フォルダー、またはフリートに対してディレクトリユーザーが必要とする初期権限を付与します。

   "アクセスロールについて".

8. ユーザーに他のフォルダー、フリート、またはロールへの追加アクセス権を付与するには、「ロールの追加」を選択し、フォルダーまたはフリート、ロールのカテゴリを選択して、ロールを選択します。

アクセスロール

NetApp Console ローカル展開アクセスロール

NetApp Consoleのローカル展開におけるIDとアクセス管理（IAM）では、リソース階層のさまざまなレベルにわたって組織のメンバーに割り当てることができる事前定義されたロールが提供されます。これらのロールを割り当てる前に、各ロールに含まれる権限を理解しておく必要があります。ロールは、プラットフォーム、アプリケーション、データ サービスのカテゴリに分類されます。

プラットフォームロール

プラットフォームロールは、NetApp Console のローカル展開管理権限（ロールの割り当てやユーザー管理を含む）を付与します。Console のローカル展開には、複数のプラットフォームロールがあります。

プラットフォームの役割	責任
"組織管理者"	組織内のすべてのフリートとフォルダへの無制限のアクセス、任意のフリートまたはフォルダへのメンバーの追加、明示的なロールが関連付けられていない任意のタスクの実行、および任意のデータサービスの使用をユーザーに許可します。このロールを持つユーザーは、適切な認証情報があれば、フォルダとフリートの作成、ロールの割り当て、ユーザーの追加、システムの管理などによって組織を管理できます。
"フォルダまたはフリート管理者"	割り当てられたフリートとフォルダーへの無制限のアクセスをユーザーに許可します。管理するフォルダーやフリートにメンバーを追加できるほか、割り当てられたフォルダーやフリート内のリソースに対して、あらゆるタスクを実行したり、あらゆるデータサービスやアプリケーションを使用したりすることができます。
"フェデレーション管理者"	ユーザーが Console を使用してディレクトリサービスフェデレーションを作成および管理できるようにすることで、ユーザーは既存のディレクトリ認証情報を使用して認証を行うことができます。
"フェデレーションビューアー"	コンソールを使用して、既存のディレクトリサービス連携を表示できるようにします。フェデレーションを作成または管理できません。

プラットフォームの役割	責任
"スーパー管理者"	ユーザーにすべての管理者権限を付与します。この役割は、Console関連の責任を複数のユーザーに分散させる必要がない小規模な組織向けに設計されています。
"スーパービューアー"	ユーザーにすべての閲覧者ロールを付与します。このロールは、Console の責任を複数のユーザーに分散させる必要がない小規模な組織向けに設計されています。

アプリケーションの役割

以下は、アプリケーションカテゴリにおける役割の一覧です。各役割は、指定された範囲内で特定の権限を付与します。必要なアプリケーションまたはプラットフォームロールを持たないユーザーは、該当するアプリケーションにアクセスできません。

アプリケーションロール	責任
"オペレーションサポートアナリスト"	監査ページなどのアラートおよび監視ツールへのアクセスを提供します。
"Storage Admin"	ストレージの健全性およびガバナンス機能の管理、ストレージリソースの検出、既存システムの変更および削除を行います。
"ストレージビューア"	ストレージの状態とガバナンス機能を表示するほか、以前に検出されたストレージリソースも表示します。既存のストレージシステムを検出、変更、または削除することはできません。
"システムヘルススペシャリスト"	ストレージ、健全性、ガバナンス機能の管理。ストレージ管理者のすべての権限を持ちますが、既存のシステムを変更または削除することはできません。

データサービスロール

以下は、データサービスカテゴリにおける役割の一覧です。各役割は、指定された範囲内で特定の権限を付与します。必要なデータサービスロールまたはプラットフォームロールを持たないユーザーは、データサービスにアクセスできません。

データサービスの役割	責任
"バックアップとリカバリのスーパー管理者"	NetApp Backup and Recoveryで任意のアクションを実行します。
"バックアップとリカバリの管理者"	ローカルスナップショットへのバックアップ、セカンダリストレージへのレプリケーション、およびオブジェクトストレージへのバックアップを実行します。
"バックアップとリカバリ復元管理者"	バックアップとリカバリでワークロードを復元します。
"バックアップとリカバリクローン管理者"	バックアップとリカバリでアプリケーションとデータをクローニングします。
"バックアップおよびリカバリビューアー"	バックアップと復元に関する情報を表示します。

データサービスの役割	責任
分類ビューア	ユーザーがNetApp Data Classificationスキャン結果を表示できるようにします。このロールを持つユーザーは、コンプライアンス情報を表示し、アクセス権限を持つリソースのレポートを生成できます。これらのユーザーは、ボリューム、バケット、またはデータベーススキーマのスキャンを有効または無効にすることはできません。Data Classification には管理者ロールがありません。
SnapCenter 管理者	アプリケーション向けNetApp Backup and Recoveryを使用して、オンプレミスのONTAPクラスターからスナップショットをバックアップする機能を提供します。このロールを持つメンバーは、次のアクションを実行できます。 * 「Backup and Recovery」＞「Applications」のすべてのアクションを実行する * 権限を持つフリートおよびフォルダー内のすべてのシステムを管理する * すべてのNetApp Consoleサービスを使用する SnapCenterにはビューア ロールはありません。

関連リンク

- "NetApp Console の ID とアクセス管理について説明します"
- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "NetApp Console 組織でメンバーを追加してロールを割り当てる"
- "NetApp Console IAM の API について"

NetApp Console ローカル展開プラットフォームのアクセスロール

プラットフォームロールをユーザーに割り当てて、NetApp Console のローカル展開の管理、ロールの割り当て、ユーザーの追加、フリートの作成、およびユーザ認証の管理に関する権限を付与します。

大規模多国籍企業における組織内役割の例

XYZ Corporationはデータのストレージ アクセスを地域別（北米、ヨーロッパ、アジア太平洋）に整理し、地域ごとの統制と一元的な監視体制を両立させています。

XYZ Corporation の Console ローカル展開における **Organization admin** は、初期組織と各地域ごとに個別のフォルダを作成します。各地域の **Folder or fleet admin** は、その地域のフォルダ内にフリート（および関連するリソース）を整理します。

Folder or fleet admin の役割を持つ地域管理者は、リソースやユーザーを追加することで、フォルダーを積極的に管理します。これらの地域管理者は、管理するフォルダやフリートを追加、削除、または名前変更することもできます。**Organization admin** は、新しいリソースに対する権限を継承し、組織全体におけるストレージ使用状況の可視性を維持します。

同一組織内では、1人のユーザーに **Federation admin** の役割が割り当てられ、組織と所属企業の IdP とのフェデレーションを管理します。このユーザーは、フェデレーション組織を追加または削除することはできますが、組織内のユーザーやリソースを管理することはできません。**Organization admin** は、フェデレーションの状態を確認したり、フェデレーションに参加している組織を表示したりするために、ユーザーに **Federation viewer** の役割を割り当てます。

以下の表は、各 Console ローカル展開プラットフォームロールが実行できるアクションを示しています。

組織管理の役割

Task	組織管理者	フォルダまたはフリート管理者
コンソールのローカル展開環境からシステムを作成、変更、または削除します（システムの追加または検出）	はい	はい
フォルダーとフリートの作成、削除を含む	はい	×
既存のフォルダとフリートの名前を変更する	はい	はい
役割を割り当ててユーザーを追加する	はい	はい
リソースをフォルダーとフリートに関連付ける	はい	はい
サポートへの登録およびコンソールからのケースの送信	はい	はい
明示的なアクセスロールに関連付けられていないデータサービスを使用する	はい	はい
監査ページと通知を表示する	はい	はい

フェデレーションロール

Task	フェデレーション管理者	フェデレーションビューアー
ディレクトリサービス統合の作成と更新	はい	×
フェデレーションとその詳細を表示する	はい	はい

スーパー管理者と閲覧者の役割

Super admin ロールは、Console 機能、ストレージ、およびデータサービスを管理するための完全なアクセス権を提供します。このロールは、管理運営やガバナンスを監督する方に適しています。一方、**Super viewer** ロールは読み取り専用アクセスを提供し、変更を加えることなく可視性を必要とする監査担当者や関係者に最適です。

組織は、セキュリティリスクを最小限に抑え、最小権限の原則に沿うために、**Super admin** アクセスの使用を控えめにすべきです。ほとんどの組織は、リスクを軽減し監査性を向上させるために、必要な権限のみを持つきめ細かなロールを割り当てるべきです。

スーパーロールの例

ABC Corporation には5人の小規模なチームがあり、データサービスおよびストレージ管理のために NetApp Console を活用しています。複数の役割を分担する代わりに、ユーザー管理やリソース構成を含むすべての管理業務を担当する2人の上級チームメンバーに **Super admin** ロールを割り当てています。残りの3人のチームメンバーには **Super viewer** ロールが割り当てられており、設定を変更する権限なしにストレージの状態とデータサービスのステータスを監視できます。

ロール	継承されたロール
スーパー管理者	• 組織管理者 • フォルダまたはフリート管理者 • バックアップとリカバリのスーパー管理者 • Storage Admin
スーパービューアー	• 組織ビューア • バックアップビューアー • ストレージビューア

NetApp Console ローカル展開における運用サポートアナリストのアクセスロール

NetApp Console のローカル展開では、ユーザーに運用サポートアナリストのロールを割り当てることで、アラートおよび監視へのアクセス権限を付与できます。

運用支援アナリスト

Task	実行可能
ストレージシステムを表示する	はい
監査ページと通知を表示する	はい
アラートの表示、ダウンロード、および設定	はい

NetApp Console ローカル展開のストレージアクセスロール

ユーザーに NetApp Console ローカル展開のストレージ管理機能へのアクセス権限を付与するには、次のロールを割り当てることができます。ユーザーには、ストレージを管理するための管理者ロール、または監視のための閲覧者ロールを割り当てることができます。

管理者は、以下のストレージリソースおよび機能に対して、ユーザーにストレージロールを割り当てることができます。

ストレージリソース：

- オンプレミス ONTAP クラスター

コンソールサービスと機能：

- ストレージの健全性機能

NetApp Console ローカル展開におけるストレージロールの例

多国籍企業であるXYZ Corporation は、ストレージエンジニアとストレージ管理者からなる大規模なチームを

擁しています。これにより、このチームは担当地域のストレージ資産を管理できる一方で、ユーザー管理やライセンス管理といった Console のコアなローカル展開タスクへのアクセスを制限することができます。

12人のチーム内で、2人のユーザーに **Storage viewer** ロールが付与され、割り当てられた Console ローカル展開フリートに関連付けられたストレージリソースを監視できるようになります。残りの9名には **Storage admin** ロールが付与されます。このロールには、ソフトウェアアップデートの管理、Console ローカル展開を通じた ONTAP System Manager へのアクセス、およびストレージリソースの検出（システムの追加）が含まれます。チームのメンバーのうち1名に **System health specialist** ロールが割り当てられ、担当地域のストレージリソースの健全性を管理できますが、システムの変更や削除はできません。この担当者は、割り当てられたフリートのストレージリソースに対してソフトウェアアップデートを実行することもできます。

組織には、ユーザー管理やライセンス管理など、Console のローカル展開のあらゆる側面を管理できる **Organization admin** ロールを持つユーザーが2名、および割り当てられたフォルダやフリートの Console のローカル展開管理タスクを実行できる **Folder or fleet admin** ロールを持つユーザーが複数います。

以下の表は、各ストレージロールが実行するアクションを示しています。

機能とアクション	**Storage Admin**	システムヘルススペシャリスト	ストレージビューア
ストレージ管理：			
新しいリソースを見つける（システムを追加する）	はい	はい	×
追加されたシステムを表示	はい	はい	×
コンソールからシステムを削除する	はい	×	×
システムを変更する	はい	×	×
システム マネージャ アクセス			
認証情報を入力できます	はい	はい	×

NetApp Backup and Recovery の役割（**NetApp Console** ローカル展開）

NetApp Console ローカル展開では、ユーザーに次のロールを割り当てて、Console 内の NetApp Backup and Recovery へのアクセス権を付与することができます。Backup and Recovery のロールを使用すると、組織内でユーザーが実行する必要のあるタスクに特化したロールを柔軟に割り当てることができます。ロールの割り当て方法は、お客様のビジネス慣行およびストレージ管理方法によって異なります。

このサービスは、NetApp Backup and Recovery に固有の次のロールを使用します。

- バックアップおよびリカバリのスーパー管理者：NetApp Backup and Recoveryですべてのアクションを実行します。
- バックアップとリカバリバックアップ管理者: ローカルスナップショットへのバックアップ、セカンダリストレージへのレプリケーション、NetApp Backup and Recovery でのオブジェクトストレージへのバックアップアクションを実行します。

- バックアップとリカバリ復元管理者：NetApp Backup and Recovery を使用してワークロードを復元します。
- バックアップとリカバリクローン管理者：NetApp Backup and Recovery を使用してアプリケーションとデータをクローニングします。
- バックアップおよびリカバリビューア：NetApp Backup and Recoveryの情報を表示できますが、アクションは実行できません。

すべての NetApp Console アクセスロールの詳細については、 "コンソールのセットアップと管理に関するドキュメント"を参照してください。

一般的なアクションに使用されるロール

以下の表は、各 NetApp Backup and Recovery ロールがすべてのワークロードに対して実行できるアクションを示しています。

機能とアクション	バックアップとリカバリのスーパー管理者	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復元管理者	バックアップとリカバリクローン管理者	バックアップおよびリカバリビューアー
ホストの追加、編集、または削除	はい	×	×	×	×
プラグインをインストールする	はい	×	×	×	×
認証情報を追加する（ホスト、インスタンス、vCenter）	はい	×	×	×	×
ダッシュボードとすべてのタブを表示する	はい	はい	はい	はい	はい
無料トライアルを開始する	はい	×	×	×	×
ワークロードの検出を開始する	×	はい	はい	はい	×
ライセンス情報を表示する	はい	はい	はい	はい	はい
ライセンスを有効化する	はい	×	×	×	×
ホストを表示	はい	はい	はい	はい	はい
スケジュール：					
スケジュールをアクティブ化	はい	はい	はい	はい	×
スケジュールを中断	はい	はい	はい	はい	×
ポリシーと保護：					

機能とアクション	バックアップとリカバリのスーパー管理者	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復元管理者	バックアップとリカバリクローン管理者	バックアップおよびリカバリビューアー
保護プランを表示する	はい	はい	はい	はい	はい
保護プランの作成、変更、または削除	はい	はい	×	×	×
ワークロードを復元する	はい	×	はい	×	×
クローンを作成、分割、または削除する	はい	×	×	はい	×
ポリシーの作成、変更、または削除	はい	はい	×	×	×
レポート：					
レポートを表示する	はい	はい	はい	はい	はい
レポートを作成する	はい	はい	はい	はい	×
レポートを削除する	はい	×	×	×	×
SnapCenter からインポートしてホストを管理：					
インポートされた SnapCenter データを表示	はい	はい	はい	はい	はい
SnapCenter からデータをインポートする	はい	はい	×	×	×
ホストの管理（移行）	はい	はい	×	×	×
設定の構成：					
ログ ディレクトリを設定	はい	はい	はい	×	×
インスタンス認証情報の関連付けまたは削除	はい	はい	はい	×	×
バケット：					
バケットを表示	はい	はい	はい	はい	はい
バケットの作成、編集、または削除	はい	はい	×	×	×

ワークロード固有のアクションに使用される役割

以下の表は、各 NetApp Backup and Recovery ロールが特定のワークロードに対して実行できるアクションを示しています。

Kubernetesワークロード

この表は、各 NetApp Backup and Recovery ロールが Kubernetes ワークロード固有のアクションに対して実行できる操作を示しています。

機能とアクション	バックアップとリカバリのスーパー管理者	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復元管理者	バックアップおよびリカバリビューアー
クラスター、ネームスペース、ストレージクラス、およびAPIリソースを表示する	はい	はい	はい	はい
新しいKubernetesクラスターを追加する	はい	はい	×	×
クラスタ構成を更新する	はい	×	×	×
管理からクラスターを削除する	はい	×	×	×
アプリケーションを表示する	はい	はい	はい	はい
新しいアプリケーションを作成して定義する	はい	はい	×	×
アプリケーション構成を更新する	はい	はい	×	×
管理からアプリケーションを削除する	はい	はい	×	×
保護されたリソースとバックアップの状態を表示する	はい	はい	はい	はい
バックアップを作成し、ポリシーを使用してアプリケーションを保護します	はい	はい	×	×
アプリの保護を解除し、バックアップを削除する	はい	はい	×	×
リカバリポイントとリソースビューアの結果を表示する	はい	はい	はい	はい
復元ポイントからアプリケーションを復元する	はい	×	はい	×

機能とアクション	バックアップとリカバリのスーパー管理者	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復元管理者	バックアップおよびリカバリビューアー
Kubernetesのバックアップポリシーを表示する	はい	はい	はい	はい
Kubernetesのバックアップポリシーを作成する	はい	はい	はい	×
バックアップポリシーを更新する	はい	はい	はい	×
バックアップポリシーを削除する	はい	はい	はい	×
実行フックとフックソースを表示する	はい	はい	はい	はい
実行フックとフックソースを作成する	はい	はい	はい	×
実行フックとフックソースを更新する	はい	はい	はい	×
実行フックとフックソースを削除する	はい	はい	はい	×
実行フックテンプレートを表示する	はい	はい	はい	はい
実行フックテンプレートを作成する	はい	はい	はい	×
実行フックテンプレートを更新する	はい	はい	はい	×
実行フックテンプレートを削除する	はい	はい	はい	×
ワークロードの概要と分析ダッシュボードを表示する	はい	はい	はい	はい
StorageGRID バケットとストレージターゲットの表示	はい	はい	はい	はい

コンソール統合とサービスの設定

NetApp Console ローカル展開を **Active Directory** と統合する

NetApp Console ローカル展開を Active Directory と統合して、ディレクトリベースのサインインとユーザー検索を実現します。ディレクトリサービスを使用してユーザーを認証し、NetApp Console ローカル展開でそれらのユーザーにアクセス権を割り当てます。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

Active Directoryと統合する場合、コンソールのローカル展開では、既存のディレクトリを通じてユーザー認証が行われます。ディレクトリユーザーを追加したら、コンソールアクセスロールを割り当てて、そのユーザーがアクセスできる範囲を制御します。

Active Directoryとの統合は、既存の制御、監査証跡、およびポリシーをコンソールのローカル展開アクセスに適用することで、コンプライアンス要件を満たすのにも役立ちます。

- Active Directoryとの統合では、フェデレーショングループの作成、ディレクトリグループの割り当ての同期、およびアクセス権の自動付与は行われません。管理者は引き続き、Console のローカル展開環境でディレクトリユーザーを組織に追加し、役割を割り当てます。
- 同時にサポートされるActive Directory統合は1つのみです。統合が設定されると、「統合を追加」ボタンは無効になります。別のディレクトリに切り替えるには、まず既存の統合を無効にするか削除してください。
- ディレクトリユーザーは、多要素認証（MFA）を設定したり使用したりしません。コンソールのローカル展開では、ローカルユーザーに対してのみMFAがサポートされます。"メンバーのセキュリティ設定を管理する方法を説明します"。

開始する前に

Active Directoryと統合する前に、以下の点を確認してください：

- Active Directoryドメインと、ディレクトリを照会できる資格情報
- LDAPサーバのアドレスとディレクトリツリーのベース識別名（DN）
- コンソールローカル展開からLDAPサーバへのネットワークアクセス（ポート389（LDAP）または636（LDAPS））
- LDAPSを使用する予定がある場合は、SSL/TLS証明書

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 「連携を追加」を選択します。
4. Active Directoryサーバーの接続詳細を入力してください：
   - 統合内容を分かりやすく表した名称。
   - **LDAP**ホスト：LDAPサーバのホスト名またはIPアドレス。複数のサーバーがある場合は、プライマリサーバーを入力してください。
   - ポート番号：LDAPの場合は389、LDAPSの場合は636。
   - *接続タイムアウト*時間（ミリ秒）。デフォルト値は1000ミリ秒です。
5. LDAPSを使用するには、*SSL/TLSを使用する*を選択してください。LDAPサーバがLDAPSをサポートしており、コンソールが必要な証明書にアクセスできることを確認してください。
6. 接続をテストしてください。失敗した場合は、LDAPホスト、ポート、ネットワーク接続、およびSSL/TLS証明書を確認してください。

7. テストが成功したら、ディレクトリとユーザーの詳細を入力します。
    - ベース**DN**バインディング：このアプリがディレクトリに接続するために使用するLDAP/ADアカウントのバインドDNを入力し、そのアカウントのバインド認証情報（パスワード）を入力します。Console はこれらの詳細情報を使用してLDAPにバインドし、接続を検証します。
    - ユーザー**DN**：ディレクトリを照会する権限を持つユーザーアカウント。例えば、 `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`。
8. 統合を保存するには、*追加*を選択してください。

終了後の操作

統合設定を保存したら、ディレクトリユーザーを組織に追加し、役割を割り当ててください。ディレクトリユーザーを追加するには、少なくとも1つのActive Directory統合を設定して有効にする必要があります。"ディレクトリユーザーの追加方法とロールの割り当て方法について説明します。"。

Active Directoryとの統合を無効化または有効化する

設定を削除せずに、ディレクトリベースの認証を一時的に停止するには、統合機能を無効にします。ディレクトリサービスを無効にすると、ディレクトリユーザーはディレクトリ経由でサインインできなくなります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 統合リストで、該当する統合を見つけ、その行のアクションメニューを選択します。
4. 統合を一時停止するには「無効にする」を選択し、復元するには「有効にする」を選択してください。

Active Directory統合を削除する

ディレクトリサービスの設定を完全に削除するには、統合を削除します。削除する前に、統合に関連付けられているディレクトリユーザーに関する警告を確認してください。これらのユーザーのアクセス権限に影響が出る可能性があります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 統合リストで、該当する統合を見つけ、その行のアクションメニューを選択します。
4. 「削除」を選択し、削除を確定してください。

LLMを接続し、**NetApp Console**のローカル展開で**NetApp Console**アシスタントを有効にする

大規模言語モデル （LLM） を NetApp Console のローカル展開に接続して、Console アシスタントと AI 支援型ストレージ管理を有効にします。

LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

設定後、ユーザーはダッシュボードから Console アシスタントを開き、アクセス モードを選択します。

- *読み取り専用*モードでは、アシスタントは変更を加えることなく質問に答え、ガイダンスを提供します。
- *読み取り/書き込み*モードでは、アシスタントはストレージ インフラストラクチャに対して操作を実行できます。変更を行う前に、確認と検証のための詳細情報が表示されます。ボリューム作成などの非同期操作の場合、ユーザーがアシスタントから確認できるジョブが作成されます。

LLMを接続するには、プロバイダーパスを選択し、エンドポイントの詳細とAPIキーを入力してから、*管理 > AIツール*でモデルを選択します。アシスタントのアクションは、ストレージポリシーとロールベースのアクセス制御の範囲内に留まります。

LLMに接続する前に必要なものを確認してください

LLMを接続する前に、以下の情報を準備してください：

- プロバイダーの種類の決定：OpenAI または OpenAI 互換。"プロバイダの選択肢について説明します。"
- 選択したプロバイダ パスに対応する有効な API キー。
- プロバイダパスのエンドポイント URL。
- 組織でプロキシ サーバまたはゲートウェイが必要な場合は、そのURLを入力してください。
- LLM プロバイダ アカウントのユーザー名またはシングル サインオン（SSO）ID（必要な場合）。
- コンソールのローカル展開から選択したエンドポイントへのネットワーク アクセス。
- 許可するアシスタント アクションのストレージ クラスとロールベースのアクセス制御。

サポートされているモデルの詳細については、"NetApp Console ローカル展開でサポートされている LLM プロバイダーとモデルについて説明します"を参照してください。

LLMをNetApp Consoleのローカル展開に接続する

LLMをConsoleのローカルデプロイメントに接続するために、プロバイダ設定、APIキー、およびモデルを入力してください。

手順

1. NetApp Console のローカル展開にログインします。
2. **Administration**（管理）**> AI Tools** を選択します。
3. メニューを選択し、次に「編集」を選択します。
4. 「プロバイダタイプ」で、プロバイダタイプを選択してください。

   "NetApp Console ローカル展開における LLM 統合について".

5. プロバイダーエンドポイントの入力を求められた場合は、選択したプロバイダーパスのエンドポイントURLを入力してください。
6. プロキシまたはゲートウェイのURLと認証情報を入力してください。
7. *ユーザー名*フィールドに、プロバイダのパスで必要な場合は、ユーザー名またはSSO IDを入力してくだ

さい。

8. *APIキー*フィールドに、選択したプロバイダーパスから取得したAPIキーを貼り付けてください。
9. リストからモデルを選択してください。
10. 設定内容を確認し、*保存*を選択してください。

    保存またはテストが失敗した場合は、プロバイダーの種類、エンドポイントURL、APIキー、および選択したモデルを確認してから、もう一度試してください。

"LLM統合に関するトラブルシューティング".

LLM統合が正しく機能することを確認します。

設定を保存したら、アシスタントの利用可否と動作を確認してください。

手順

1. コンソールアシスタント ボタンが NetApp Console ローカルデプロイメントダッシュボードに表示されていることを確認してください。
2. アシスタントを*読み取り専用*モードで開き、基本的なクエリを実行します。
3. アシスタントを **Read/write** モードで開き、ストレージを変更する操作を実行する前にユーザーの確認が必要であることを確認してください。
4. アクションワークフローを必要とするユーザーが、必要なロールベースのアクセス制御を持っていることを確認してください。

検証が完了すると、ユーザーはダッシュボードからコンソールアシスタントを開き、タスクを平易な言葉で説明できるようになります。使用例とエンドユーザワークフローについては、"NetApp Console アシスタントを使用する"を参照してください。

認証情報を保護し、**LLM**の使用状況を監視する

- 可能な限り、Console のローカル展開統合には専用の API キーを使用してください。
- 組織のポリシーに従ってAPIキーをローテーションしてください。
- AIツールの設定を編集できるユーザーを、必要な管理者ロールのみに制限します。
- プロバイダー側のAPI使用状況とアラートを監視して、異常なアクティビティやコストの急増を追跡します。

NetApp Consoleローカルデプロイにおける**LLM**統合のトラブルシューティング

NetApp Console のローカル展開における一般的な LLM 統合の問題を診断および解決するには、このクイックトリアージフローを使用してください。

LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

セットアップが完了していない場合は、"LLMを接続してNetApp Consoleアシスタントを有効にする"を参照してください。

LLM統合の問題を迅速にトリアージする

1. 管理 ＞ **AI Tools** でAI Toolsの設定を確認してください。

   プロバイダーの種類、エンドポイント URL、API キー、選択したモデル、および送信ネットワーク アクセスを確認してください。

2. ダッシュボード上でアシスタントの可用性を確認してください。

   想定されるユーザーおよび組織に対して、**Console assistant** ボタンが表示されることを確認してください。

3. 実行時動作を検証する。

   単純な読み取り専用リクエストを実行し、プロバイダーエンドポイントへの到達可能性、モデルの可用性、およびプロバイダーサービスの健全性を確認します。

症状別にトラブルシューティングを行う

現象	考えられる原因	チェックする項目	次のアクション
AI Tools での保存またはテストの失敗	設定または接続の不一致	プロバイダーの種類、エンドポイントURL、APIキーの形式、選択されたモデル、およびアウトバウンドアクセス	検証に失敗した値を修正して、再度保存してください。
「Console assistant」ボタンがありません	統合状態が不健全、組織の不一致、またはRBACの不一致	AI ツールの保存、統合ステータス、現在の組織、および想定されるアクセスロールが正常に完了しました	セッションを更新し、既知の正常な管理者アカウントで確認してください。
アシスタントは起動するが、リクエストが失敗する	プロバイダーまたはランタイムパスの問題	エンドポイントへの到達可能性、そのエンドポイントにおけるモデルの可用性、プロバイダーの制限、および一時的なプロバイダーの状態	エンドポイント/モデルの不一致またはプロバイダー側の制限の問題を修正した後、再試行してください。
アシスタントの応答が遅い、または一貫性がない	プロンプトサイズ、エンドポイントのパフォーマンス、またはネットワーク/プロキシの不安定性	短時間の簡易テスト、プロバイダーサービスの健全性、ネットワーク/プロキシの安定性	プロンプトを短くするか、別のサポートされているモデルを試すか、ネットワークまたはプロキシのルーティングを安定させる

LLM クレデンシャルの漏洩または不正使用への対応

APIキーの漏洩または不正使用が疑われる場合：

1. プロバイダーシステムに登録されている既存のAPIキーを無効にしてください。
2. 新しいAPIキーを作成します。
3. 「管理」＞「AI Tools」でキーを更新してください。

4. 読み取り専用のアシスタントテストを使用して、再接続が成功したことを確認してください。

NetApp Console ローカル展開で通知配信チャネルを設定する

NetApp Console のローカル展開では、メールや Webhook など、アラート通知用の複数のチャネルを設定できます。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

デフォルトでは、コンソールのローカル展開では、組み込みの通知システムを通じて通知が表示されます。追加の配信チャネルを設定することで、ワークフローに最適な方法で通知を受け取ることができます。

すべての通知を同じチャネルで送信することも、通知の種類ごとに異なるチャネルを使用することもできます。例えば、緊急のストレージアラートはメールで送信し、その他のアラートトラフィックはWebhookを介してサードパーティの監視ツールにルーティングするといったことが可能です。

通知配信チャネルを設定した後、通知ルールを設定し、それらを異なるチャネルに割り当てることができます。"通知ルールの設定方法を確認します"。

メールサーバーの設定

メールサーバーを設定すると、コンソールのローカル展開では、通知、アラート、およびユーザー招待がそのメールサーバー経由で送信されます。コンソールのローカル展開では、SMTPメールサーバーがサポートされており、既存の社内メールサーバー、またはサードパーティのメールサービスを使用できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. メールサーバーの接続情報を入力してください：
   - 送信者名と送信者のメールアドレスを追加してください。
   - **SMTP** ホスト：SMTP サーバーのホスト名または IP アドレス。複数のサーバーがある場合は、プライマリサーバーを入力してください。
   - 「接続セキュリティ」ドロップダウンリストから接続プロトコルを選択してください。ポートは自動的に設定され、読み取り専用です：STARTTLS を使用する SMTP の場合は 25、SMTPS の場合は 465。

     SMTPS（ポート465）は即座に暗号化された接続を確立するため、セキュリティが重視される環境での使用が推奨されます。STARTTLS（ポート25）は暗号化されていない接続からアップグレードし、暗号化のネゴシエーションが失敗した場合は暗号化されていない送信にフォールバックする可能性があります。
5. テストメール を選択すると、指定した受信者にテストメールが送信されます。
6. テストが成功したら、*保存*を選択して設定を保存します。

   テストが失敗した場合は、入力した設定を再確認し、Console のローカル展開がメールサーバーへのネットワーク アクセスを持っていることを確認してください。

メールサーバーの設定を更新する

別のメールサーバーを使用したい場合は、既存のメールサーバー設定を更新できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. 既存の設定をクリアするには、*フィールドをクリア*を選択してください。
5. メールサーバーの新しい接続情報を入力してください。
6. テストメール を選択すると、指定した受信者にテストメールが送信されます。
7. テストが成功したら、*保存*を選択して新しい設定を保存します。

   テストが失敗した場合は、入力した設定を再確認し、Console のローカル展開がメールサーバーへのネットワーク アクセスを持っていることを確認してください。

メールサーバーの設定を削除する

コンソールローカル展開でメールを送信する必要がなくなった場合は、メールサーバーの設定を削除できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. 既存の設定をクリアするには、*フィールドをクリア*を選択してください。
5. 「保存」を選択すると、クリアした設定が保存され、Console のローカル展開からメールサーバーの設定が削除されます。

ウェブフックを設定する

コンソールのローカルデプロイメントから他のツールやサービスに通知を送信するように、Webhookを設定します。複数のWebhookを設定でき、それぞれ異なるエンドポイントを指すように設定できます。例えば、SIEMと、オンコールページングサービス用などです。

Webhookを作成すると、ストレージ管理者ロールを持つユーザーは、それを特定のアラートルールに割り当てることができます。例えば、重要なアラートはメールで送信しつつ、すべてのアラートをWebhook経由でサードパーティの監視ツールに送信するといったことが可能です。

> コンソールのローカル展開では、WebhookエンドポイントへのアクセスコントロールはEnforceされません。エンドポイントURLにアクセスできるユーザーまたはシステムは、アラートデータを受信します。受信アプリケーションへのアクセスは、そのアプリケーション独自のアクセス制御を通じて、承認されたユーザーのみに制限されるようにしてください。

開始する前に

コンソールのローカル展開がネットワーク経由で受信アプリケーションに到達できることを確認し、エンドポ

イントURL、HTTPメソッド、およびそのアプリケーションが必要とする認証情報や証明書の詳細情報を収集します。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「Webhook integration」セクションで、「Configure」を選択します。
4. ウェブフックに必要な詳細情報を入力してください：
   - ウェブフックを表す分かりやすい名前。
   - 受信側アプリケーションから提供されるエンドポイントURL。
   - HTTPメソッド
   - オプション：PEM形式の自己署名証明書。
   - 必要なヘッダーまたはシークレット（認証クレデンシャル）。
   - ウェブフックを送信する際に使用するフォーマット。JSONとOTEL（OpenTelemetry）がサポートされています。

     汎用的なWebhookやカスタムRESTエンドポイントにはJSONを使用してください。GrafanaなどのOpenTelemetryシグナルをネイティブに使用するオブザーバビリティプラットフォームや、その他のOpenTelemetry互換コレクターにはOTELを使用してください。
5. 「Test webhook」を選択して、Webhook 接続をテストし、Console のローカル展開が受信アプリケーションにメッセージを正常に送信できることを確認してください。
6. テストが成功したら、*保存*を選択してウェブフックを作成します。

   ウェブフックを保存すると、アラート配信オプションなど、ウェブフックがサポートされている場所をユーザーが選択できるようになります。"アラートルールを作成し、アラート配信のための Webhook を割り当てる方法について説明します。"

NetApp Console を使用する

NetApp Console ローカル展開にログインする

組織管理者からコンソールローカル展開の組織ユーザーアカウントへの招待を受けた後、NetApp Console ローカル展開にサインインできます。ログインするには、ログインに関連付けられているメールアドレスを使用します。

ログインしてもリソースが表示されない場合は、組織の管理者に問い合わせてください。"組織の管理者に問い合わせてください".

手順

1. Webブラウザを開き、Console のローカル展開がインストールされている IP アドレスにアクセスしてください。
2. 「ログイン」ページで、ログインに使用しているメールアドレスを入力してください。

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に求められます。

   - 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

     - MFAが有効になっている場合：パスワードを入力した後、TOTPコード（認証アプリから取得）を入力するか、リカバリコードを使用するように求められます。
     - 復旧コードを使用してサインインする場合は、復旧コードの入力画面でUIに表示される順序でコードを使用してください。

   +

   - メールアドレスとパスワードを使用したActive Directoryアカウント

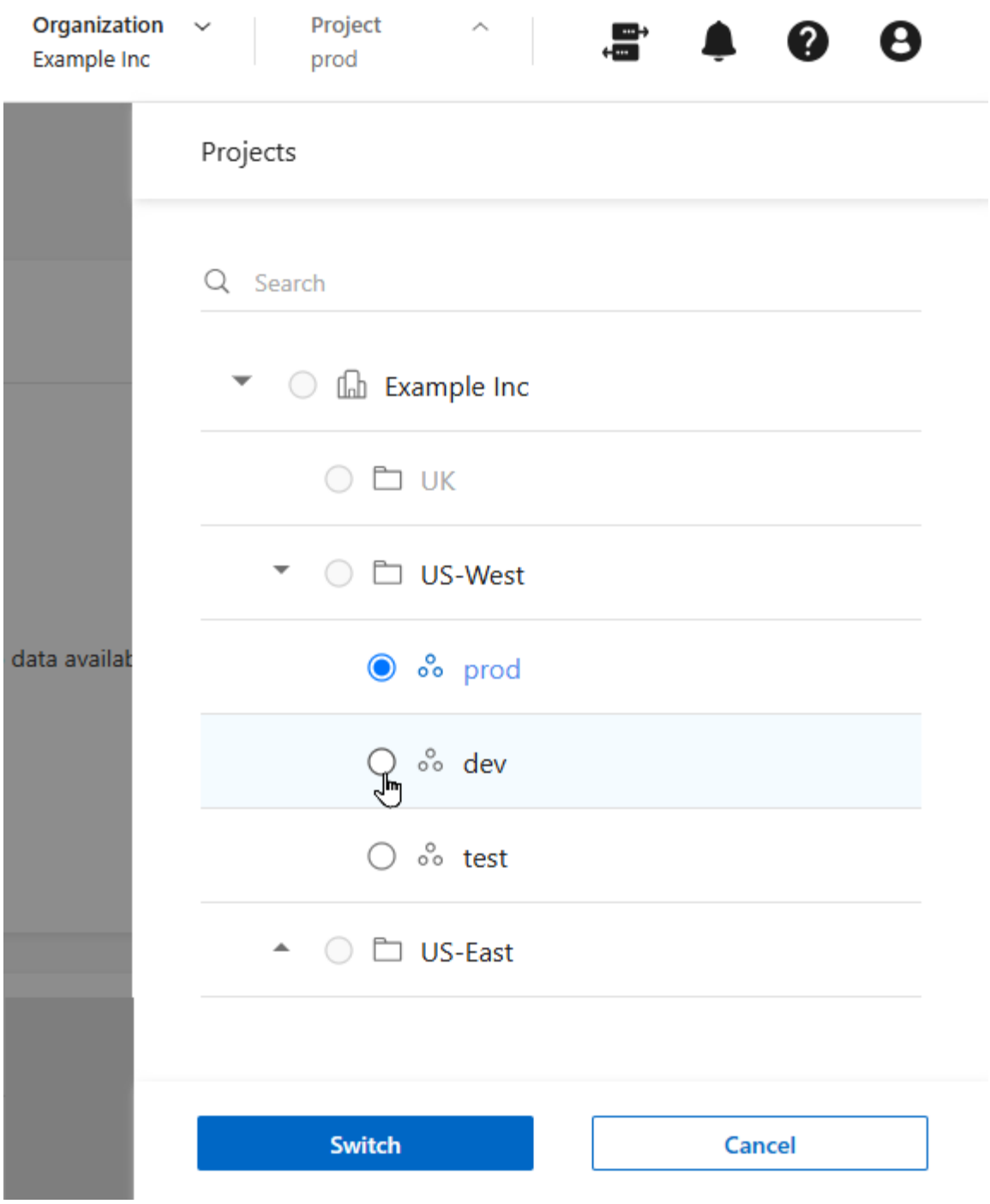
NetApp Console ローカル展開でフリートを切り替える

NetApp Console のローカル展開において、複数のフリートにアクセスできる場合は、いつでも切り替えることができます。

「IDとアクセス」ページを表示している間は、別のフリートに切り替えることはできません。

手順

1. コンソールのローカル展開の上部ヘッダーで、*スコープ*を選択します。
2. 組織内のフリートを参照し、使用するフリートを選択してから、*切り替え*を選択してください。



NetApp Console ローカル展開のユーザー設定を管理する

NetApp Console のローカル展開では、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、Console のローカル展開プロファイルを変更できます。

表示名を変更する

コンソールのローカル展開における表示名を変更できます。この表示名は、他のユーザーに対してお客様を識別するために使用されます。ユーザー名やメールアドレスは変更できません。

手順

1. コンソールのローカル展開画面の右上隅にあるプロファイルアイコンを選択すると、ユーザー設定パネルが表示されます。
2. 自分の名前の横にある **Edit** アイコンを選択してください。
3. 「名前」フィールドに新しい表示名を入力してください。

多要素認証を設定する

NetAppConsole ローカル展開へのログイン時に2つ目の認証方法を必須とすることでセキュリティを強化するために、多要素認証（MFA）を設定します。

NetApp Support Site からサインインするユーザーは、MFA を有効にできません。これがお客様に当てはまる場合、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をAPIアクセスに使用している場合は、MFAを有効にしないでください。多要素認証が有効になっているユーザーアカウントでは、APIへのアクセスが停止されます。すべてのAPIアクセスにはサービスアカウントを使用してください。

アカウントが認証にActive Directoryまたはその他の統合ディレクトリサービスを使用している場合、Console のローカル展開を通じてアカウントのMFAを設定することはできません。

開始する前に

- お使いのデバイスには、Google AuthenticatorやMicrosoft Authenticatorなどの認証アプリを既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、または復旧コードを紛失した場合は、Console管理者にお問い合わせください。

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すると、ユーザー設定パネルが表示されます。
2. **Multi-Factor Authentication** の見出しの横にある **Configure** を選択します。
3. 画面の指示に従って、アカウントの多要素認証を設定してください。
4. 完了すると、復旧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てください。これらのコードは安全な場所に保管してください。認証アプリへのアクセスを失った場合は、復旧コードが必要になります。

   復旧コードを使用してサインインする必要がある場合は、復旧コードの入力画面でUIに表示される順序でコードを使用してください。

   MFAを設定すると、コンソールのローカル展開では、ログインするたびに認証アプリからワンタイムコードを入力するよう求められます。

MFA 回復コードを再生成する

復旧コードは一度しか使用できません。紛失した場合は、新しいコードを作成してください。

手順

1. コンソールのローカル展開画面の右上隅にあるプロファイルアイコンを選択すると、ユーザー設定パネルが表示されます。
2. 「Multi-Factor Authentication」ヘッダーの横にある ••• を選択します。
3. 「リカバリーコードの再生成」を選択します。
4. 生成された復旧コードをコピーし、安全な場所に保存してください。

MFA設定を削除する

MFAを削除すると、次回のサインイン時の2段階認証が不要になります。MFAを再度使用するには、ユーザー設定から再度設定する必要があります。

認証アプリまたは復旧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 の設定をリセットする必要があります。

手順

1. コンソールのローカル展開画面の右上隅にあるプロファイルアイコンを選択すると、ユーザー設定パネルが表示されます。
2. 「Multi-Factor Authentication」ヘッダーの横にある ••• を選択します。
3. *Delete*を選択します。

組織の管理者に連絡してください。

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。

「管理者への連絡」機能を使用するには、ブラウザにデフォルトの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. コンソールのローカル展開画面の右上隅にあるプロファイルアイコンを選択すると、ユーザー設定パネルが表示されます。
2. 組織の管理者にメールを送信するには、*管理者に連絡*を選択してください。
3. 使用するメールアプリケーションを選択してください。
4. メールを完成させて、*送信*を選択してください。

ダークモード（ダークテーマ）を設定する

コンソールのローカル展開をダークモードで表示するように設定できます。

手順

1. コンソールのローカル展開画面の右上隅にあるプロファイルアイコンを選択すると、ユーザー設定パネルが表示されます。
2. ダークテーマ のスライダーを動かして有効にしてください。

NetApp Console のローカル展開で NetApp Console アシスタントを使用する

NetApp Console のローカル展開で NetApp Console アシスタントを使用して、ストレージを管理したり、自然言語で回答を取得したりできます。必要なことを平易な言葉で説明すると、NetApp Console のローカル展開がストレージポリシーとロールベースアクセスの範囲内でそれを実行します。

> LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

アシスタントの操作は、割り当てられたロールベースのアクセス権によって制限されます。"アクセスロールについて"。

コンソールアシスタントでできることを確認する

コンソールアシスタントは、NetApp Console ローカル展開への自然言語インターフェースです。質問をしたり、タスクを説明したりすると、回答または提案されたアクションが返されます。このアシスタントは以下の機能を提供します：

- ストレージのプロビジョニング ワークロードを平易な言葉で説明します。アシスタントはストレージクラスと配置場所を推奨し、詳細を確認後、ボリュームまたはLUNを作成します。例えば、特定の容量を持つCIFSボリュームを作成するように指示します。アシスタントは、クラスターとストレージ仮想マシン（SVM）を識別し、必要なパラメーターを入力し、ストレージをプロビジョニングします。
- 検索してガイダンスを取得 ストレージ環境に関する質問をしたり、コンソールのローカル展開機能を見つけたり、NetApp ドキュメントおよび現在のフリート状態からコンテキストに応じた回答を取得したりできます。
- アラートの調査 アシスタントにアクティブなアラートを調査するように依頼します。問題点を分析し、解決策を提案するか、お客様の確認を得た上で修復措置を実行します。

アシスタントは、コンソールのローカル展開で管理者が設定したLLMエンドポイントにのみリクエストを送信します。ストレージ変更アクションを実行する前に確認を要求し、すべてのアクションはお客様のアカウントに割り当てられたロールベースのアクセス制御に従います。

コンソールアシスタントが使用できることを確認してください。

- 組織管理者またはスーパー管理者は、大規模言語モデル（LLM）をコンソールのローカル展開に接続することにより、コンソールアシスタントを有効にする必要があります。ダッシュボードに「コンソールアシスタント」ボタンが表示されない場合は、管理者に有効化を依頼してください。詳細については、"LLMを接続してNetApp Consoleアシスタントを有効にする"を参照してください。
- アシスタントに実行させたい操作に必要なロールベースのアクセス制御が設定されていることを確認してください。

コンソールアシスタントに質問するか、アクションをリクエストしてください。

コンソールアシスタントを開き、アクセスモードを選択して、リクエスト内容を説明するプロンプトを入力します。

手順

1. NetApp Console のローカル展開ダッシュボードで、「コンソールアシスタント」ボタンを選択します。
2. アクセスモードを選択してください：
   - 変更を加えることなく質問やガイダンスを受けるには、閲覧専用 を選択してください。
   - アシスタントがストレージインフラストラクチャ上で操作できるようにするには、「読み取り/書き込み」を選択します。
3. 質問やタスクの内容を説明するプロンプトを入力し、*送信*を選択してください。

   例：`Create a 10GiB volume for home directories named home, and share it with Everyone set to FULL_CONTROL.`
4. アシスタントの回答を確認してください。
   - 質問に対して、アシスタントはお客様が対応できる回答を返します。
   - 操作を行う際、アシスタントは推奨される操作を表示し、権限レベルなどの不足している詳細情報を尋ね、その後、実行前に確認を求めます。
5. 操作を確認してください。ボリューム作成などの非同期操作の場合、アシスタントはリクエストを完了するためのジョブを作成します。
6. 依頼内容を確認するには、アシスタントにお問い合わせください。例えば、 `Let me know when the job completes`と入力すると、アシスタントは現在のステータスを返します。

NetApp Console でストレージを管理する

NetApp Console ローカルデプロイにおけるフリート管理について説明します

NetApp Consoleのローカル展開におけるフリート管理とは、ストレージシステムを論理グループに整理することで、一貫したポリシーの適用、アクセス制御、および関連するクラスター全体のヘルス状態の監視を行うプラクティスです。フリート管理を使用すると、各クラスターを個別に管理する代わりに、フリートを共通のリソースプールとして扱い、データストレージの目標をサポートできます。

ストレージ環境が拡大するにつれて、個々のクラスターを管理することは非現実的になります。フリート管理は、関連するシステムを体系的にグループ化し、責任を委任し、すべてのクラスターが同じ基準で運用されるようにすることで、この問題を解決します。

フリート管理が重要な理由

フリート管理は、以下の3つの主要な課題に対処します：

- 抽象化による簡素化 - フリート管理は、個々のストレージインフラストラクチャの管理の複雑さを抽象化します。クラスターごとに設定を行う代わりに、ストレージ環境全体を統一的に管理することで、運用上の負担と意思決定の負担を軽減できます。
- 一貫性と拡張性 - 明確な組織体制がないと、異なるチームが類似のワークロードに対して異なる決定を下し、断片化された構成につながります。フリート管理機能を使用すると、数十ものシステムに同時に標準を適用できるため、新しいワークロードがチームやフリート全体で同じ基準から開始されることが保証されます。
- ガバナンスと管理 - チームが大きくなるにつれて、誰が何を管理できるかについて明確な境界線が必要に

なります。フリート管理は、組織構造とアクセス制御を通じてこれらの境界を設定し、ストレージに関する決定が統制され、監査可能であることを保証します。

フリートによるリソースの整理方法

組織のリソース階層は、フォルダーとフリートで構成されています。

階層構造とアクセスモデルの詳細については、"NetApp Console ローカル展開におけるフォルダーとフリートについて"を参照してください。

- 組織 - お客様の会社を表す最上位レベル。
- 「フォルダー」：関連するフリートを整理するのに役立ちます。たとえば、リージョンやビジネスユニットごとにフォルダーを作成し、各フォルダー内にフリートを作成できます。フォルダーには、他のフォルダーやフリートを含めることができます。フォルダーレベルでロールを割り当てると、メンバーはそのフォルダー内のすべてのフリートに対してそのロールを継承します。
- フリート - 管理しているストレージシステムをグループ化します。ストレージシステムをフリートに関連付け、メンバーをフリートに割り当てることでアクセス権を付与します。

> フォルダは組織管理ツールであり、組織管理者、フォルダ管理者、フリート管理者などのIAM権限を持たないメンバーには表示されません。メンバーはフォルダではなく、フリートにアクセスします。

一般的なフリート編成パターン

フリートの編成方法は、運用モデルによって異なります。

- 環境別 - 本番環境、開発環境、テスト環境のワークロード用に個別のフリートを作成します。これにより、本番環境のストレージはより厳格なポリシーの下で管理される一方、下位環境ではより高い柔軟性が確保されます。
- 事業部門別 - 財務、エンジニアリング、人事など、特定の部門にサービスを提供するクラスターを専用のフリートにまとめます。そうすることで、他のフリートを公開することなく、その事業部門内のチームメンバーにストレージ管理の責任を割り当てることができます。
- 場所またはデータセンター別 - クラスターが複数のサイトに分散している場合、場所別に整理することで、サイトレベルの健全性を監視したり、地域固有のポリシーを適用したり、サイトごとの容量消費量を追跡したりできます。
- アプリケーション層別 - データベース、ファイル共有、仮想マシンなど、特定の種類のワークロードをホストするクラスターをグループ化することで、そのワークロードタイプに合わせて調整された一貫した標準をフリート全体に適用できます。

> フォルダを使用して、さらに整理のレベルを追加します。例えば、地域ごとにフォルダを作成し、各地域フォルダ内に環境ベースのフリートを作成します。

フリート管理がアクセス制御を可能にする方法

フリートとフォルダは、ユーザーアクセスと管理責任の境界として機能します。

- フォルダレベルのアクセス - フォルダレベルで役割を割り当てると、メンバーはそのフォルダ内のすべてのフリートとリソースに対してその役割を継承します。これにより、組織全体へのアクセス権を付与することなく、管理上の責任を委任できます。

- フリートレベルのアクセス - フリートレベルで役割を割り当てると、メンバーはそのフリート内のストレージシステムにのみアクセスできます。これにより、インフラストラクチャの無関係な部分を公開することなく、ストレージ管理をチームメンバーやアプリケーション所有者に委任できます。

コンソールローカル展開では、フリートレベルの健全性とパフォーマンスの監視機能が提供されるため、フリート内のすべてのクラスターの状態を単一のビューで確認し、問題を早期に特定して、ワークロードに影響が出る前に対応できます。

ストレージ管理の仕組み

ストレージ管理とは、ストレージの標準を定義し、それを一貫して適用し、ワークロードが長期にわたって整合性を保つように運用する実践のことです。Console のローカル展開では、これらの標準はストレージクラスポリシーとストレージクラスとして表現され、フリートごとにスコープが設定され、RBAC と監査ログによって管理されるプロビジョニングワークフローを通じて適用されます。

コンソールローカル展開では、4つの概念が1つのワークフローに統合されます：

- *フリート*は、ストレージを管理する範囲を定義します。フリートとは、システムをグループ化することで、アクセスを制御し、標準を一貫して適用し、リソースを単位として管理できるようにするものです。
- *ストレージクラスポリシー*は、再利用可能な構成要素（パフォーマンス、容量、セキュリティ、データ保護）として標準を定義します。
- *ストレージクラス*はワークロードの意図を表します。ストレージクラスとは、1つ以上のポリシーから構成される、名前付きのテンプレートのことです。
- *プロビジョニングワークフロー*は、ガードレール内でストレージを作成します。ワークフローによって構成決定の方法は異なりますが、いずれの場合もストレージクラスを適用でき、RBACと監査ログによって管理されます。

プロビジョニングのアプローチ

コンソールのローカル展開では、3つのプロビジョニング方式がサポートされており、いずれもRBAC、監査ログ、およびストレージクラス標準によって管理されます。

- 手動プロビジョニング - 対象システムを選択し、構成の詳細を直接指定します。システム選択と構成を明示的に制御する必要がある場合に使用します。
- 自動プロビジョニング - ワークロードの入力値を指定し、必要に応じてストレージクラスを選択します。NetApp Console のローカル展開では、最適な配置が推奨され、クラス駆動型の設定が適用されるため、手動での決定が軽減されます。
- **AI**支援（エージェント型）プロビジョニング - 必要なものを自然言語で説明します。Console のローカル展開では、RBAC とストレージクラスによって制約されたプランが提案され、お客様が確認して承認した後にのみプロビジョニングが実行されます。

次のステップ

- ストレージ規格を理解するには、"NetApp Console ローカル展開におけるストレージクラスとポリシーについて"を参照してください。
- フリートの作成と管理については、"フォルダとフリートを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"

- "AI支援によるストレージの提供"

ストレージの動作を標準化する

NetApp Console ローカル展開におけるストレージクラスとポリシーについて

ストレージクラスとは、ストレージがどのように動作するべきかを定義する、再利用可能なテンプレートです。ストレージクラスを使用してストレージをプロビジョニングする場合、NetApp Console のローカル展開では、管理者がワークロードごとに個別の構成決定を行う必要なく、そのクラスにエンコードされた標準が自動的に適用されます。

ストレージクラスは、ストレージ動作の個々の側面を定義するストレージクラスポリシーに基づいて構築されます。これらを組み合わせることで、組織のストレージ標準を一度設定すれば、それをすべてのシステムで一貫して適用できるようになります。

ストレージクラスポリシーとは

ストレージクラスポリシーは、ストレージの動作の一側面を定義します。ポリシーは、ストレージクラスを作成するために組み合わせる、再利用可能な構成要素です。

一般的なポリシーの種類は以下のとおりです：

- パフォーマンス ポリシー - レイテンシー ターゲット、IOPS、またはスループット要件を定義します。
- 容量ポリシー - プロビジョニングモード、しきい値アラート、または拡張制限を定義します。
- セキュリティポリシー - 暗号化、コンプライアンス、またはアクセス制御の要件を定義します。
- データ保護ポリシー - スナップショットのスケジュール、レプリケーションのターゲット、または保持期間を定義します。

ポリシーは個別に定義し、ストレージクラスを構築する際にそれらを組み合わせます。これにより、複数のクラスで同じパフォーマンス ポリシーを再利用したり、容量ポリシーを 1 か所で更新して、そのポリシーを使用するすべてのクラスにその変更を適用したりすることができます。

ストレージクラスとは

ストレージクラスとは、1つ以上のポリシーから構成される、名前付きのテンプレートのことです。これは、特定の種類のワークロードに対する組織のストレージ標準を表すものです。

例えば、ハイパフォーマンス、高可用性、厳格な保護ポリシーを組み合わせた **Production Database** ストレージクラス、または適度なパフォーマンス、柔軟な容量、基本的な保護ポリシーを組み合わせた **Development File Share** ストレージクラスを作成することができます。

ストレージ管理者は、企業要件を反映させるためにストレージクラスを定義します。プロビジョニング活動は、手動で行う場合でも、ガイド付きワークフローを通じて行う場合でも、自動化によって行う場合でも、管理者が承認したクラスのライブラリからデータを取得します。

ストレージクラスが標準をどのように適用するか

ストレージをプロビジョニングする際は、個々の設定を構成するのではなく、ストレージクラスを選択します。Console のローカル展開では、そのクラスのポリシーを使用して、フリート内のどのクラスターがワークロードをサポートする容量とパフォーマンスの余裕を持っているかを特定し、最適な配置オプションを推奨

し、プロビジョニング時にクラス駆動型の設定を自動的に適用します。

プロビジョニング後、NetApp Console のローカルデプロイメントは、各ワークロードをストレージクラスの標準に照らし合わせて継続的に評価します。

ストレージクラスの変更とコンプライアンス

ワークロードがストレージクラスの意図と一致しなくなった場合、Console のローカルデプロイメントは、調査と修復のためにそのワークロードにフラグを立てます。

問題は2つのカテゴリーに分類されます：

- 構成のずれ：ストレージクラスポリシーによって管理されるストレージ設定が、意図した構成と一致しなくなりました。これは、ONTAP クラスターで直接変更が行われた場合、または標準のプロビジョニングワークフロー外で変更が行われた場合に発生する可能性があります。
- パフォーマンス不適合：ワークロードの実行時動作がストレージクラスのパフォーマンス要件を満たさなくなりました（たとえば、QoS 制限付近での持続的な負荷、またはテールレイテンシの増加など）。

分析ビューでは、何が変わったのか、そしてなぜ変わったのかが説明されます。コンプライアンスを回復するために、ガイド付きの是正措置（例えば、**Fix it** など）が利用できる場合があります。一部の修復策はそのまま適用できますが、意図した動作を復元するためにワークロードを別のストレージクラスに調整する必要がある場合もあります。

調査する場所

通常、以下のいずれかの場所からドリフトやコンプライアンス違反を調査できます（利用可能かどうかは、デプロイメントと権限によって異なります）：

- ストレージクラス： ドリフト / コンプライアンス
- アラート： 分析

手順の詳細については、ストレージクラスのずれを修正するを参照してください。

エンドツーエンドのワークフロー

以下の手順では、ストレージクラスを使用して環境内のストレージを標準化および管理するプロセスについて説明します。

1. ストレージクラスポリシーの作成 - ポリシーは、ストレージ動作の個々の側面（パフォーマンス目標、容量設定、セキュリティ要件、データ保護スケジュール）を定義します。ストレージクラスを構築する前に、ポリシーを作成してください。
2. ストレージクラスの作成 - 該当する各カテゴリから1つのポリシーを組み合わせてストレージクラスを作成します。事前定義されたストレージクラスを使用するか、組織の基準に合わせてカスタムのストレージクラスを作成することができます。
3. ストレージクラスをフリートに関連付ける - ストレージクラスを作成したら、プロビジョニングとコンプライアンス監視に使用するフリートに関連付けます。
4. ストレージクラスを使用してストレージをプロビジョニングする - ボリュームまたは LUN をプロビジョニングする際に、個々の設定を構成する代わりにストレージクラスを選択します。Console のローカル展開では、クラスを使用して最適なクラスタ配置を推奨し、クラスで定義された設定でプロビジョニングを行います。
5. ワークロードのずれを監視する - Console のローカル展開では、各ワークロードをストレージクラスにエ

ンコードされた標準と照らし合わせて継続的に評価します。設定のずれやパフォーマンスの不適合が発生した場合、その問題にフラグが付けられ、アラートが発生する可能性があります。

6. ドリフトを修復してコンプライアンスを回復する - ドリフトまたはパフォーマンスの非コンプライアンスが検出された場合、ガイド付き手順に従って問題を手動で修正したり、Console のローカル展開で一般的なドリフト状態を自動的に解決したり、設定を変更する必要がある場合はワークロードをストレージ クラスから切り離したりできます。

ストレージクラスがフリートとどのように連携するか

ストレージクラスはフリートに関連付けられています。ストレージクラスをフリートに関連付けると、そのクラスはフリート内のすべてのプロビジョニングで使用できるようになります。これにより、フリート内でプロビジョニングされるすべてのワークロードが同じ標準に従うことが保証され、フリートは関連するクラスター全体で一貫したストレージ動作を適用するための主要な手段となります。

フリートの整理方法の詳細については、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。

次のステップ

- フリート編成を理解するには、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。
- ポリシーとストレージ クラスを作成するには、"ストレージクラスとポリシーを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"
- "AI支援によるストレージの提供"
- ドリフトの分析と修正については、"ストレージクラスのずれを修正する"を参照してください。

NetApp Console ローカル展開におけるストレージクラスポリシーについて

ストレージクラスポリシーは、ストレージクラスを構築するために使用する構成要素です。各ポリシーは、ストレージ動作の特定の側面を制御します。ポリシーをストレージクラスに組み合わせると、再利用可能なテンプレートが作成されます。このテンプレートは、NetApp Console のローカル展開がプロビジョニング時に自動的に適用し、ワークロードのライフサイクル全体を通じて継続的に監視します。

ポリシーをビルディングブロックとして活用する

ストレージクラスは1つ以上のポリシーで構成され、それぞれのポリシーはストレージ動作の異なる側面を規定します。ストレージ管理者は、パフォーマンス要件、容量のしきい値、データ配置ルールといったエンタープライズ標準をポリシーとして定義し、それらのポリシーをストレージクラスのテンプレートにまとめます。ワークロードがストレージクラスを使用してプロビジョニングされると、そのクラスのすべてのポリシーが継承されます。この設計では、標準を定義する責任とプロビジョニングの作業を分離することで、個別の構成を決定することなく、自動化されたワークフローによってストレージを一貫してプロビジョニングできます。

ストレージクラスポリシーの種類

NetApp Console のローカル展開には、ストレージクラスを構築するために使用できる4種類のポリシーが含まれています：

パフォーマンスポリシー

パフォーマンスポリシーは、ワークロードに対して、期待IOPS/TB、ピークIOPS/TB、絶対最小IOPS、および期待レイテンシの目標値を設定します。NetApp Console のローカルデプロイメントでは、これらの値を使用して、プロビジョニング時に十分な余裕のあるクラスターを推奨し、プロビジョニング後にIOPSまたはレイテンシの変動を検出します。

容量ポリシー

容量ポリシーは、ボリュームがスペースをどのように消費および管理するかを制御します。スペース リザベーション（thick、thin、またはシステムデフォルト）、自動拡張動作、FabricPool 階層化、およびNASワークロードを FlexVol または FlexGroup ボリュームとしてプロビジョニングするかどうかを設定します。

セキュリティポリシー

セキュリティポリシーは、ワークロードに対する暗号化、ランサムウェア対策、およびFIPS要件を設定します。各属性は必須値を設定することも、「any」のままにしてシステムデフォルト値を受け入れることもできます。

データ保護ポリシー

データ保護ポリシーは、ポリシーを使用するワークロードが一貫したバックアップスケジュールを確保できるように、各間隔で保持するスナップショットの数を設定します。

デフォルト ポリシー

コンソールのローカル展開には、4つのポリシータイプすべてにわたるシステム定義ポリシーが含まれます。これらのポリシーは、ストレージクラスを作成する際にそのまま使用することも、組織の要件に合わせてカスタマイズしたポリシーを作成する際の出発点としてコピーすることもできます。

パフォーマンスポリシー

Name	**Type**	想定**IOPS/TB**	ピーク**IOPS/TB**	絶対最小**IOPS**	想定される遅延時間（ミリ秒）	サマリ
最高レベル（データベース データ用）	システム定義	12,288	24,576	2,000	1	持続的に高いIOPSとミリ秒以下のレイテンシを必要とするトランザクショナルデータベースのデータボリュームに使用します。
最高レベル（データベース ログ用）	システム定義	22,528	45,056	4,000	1	書き込みボトルネックを防ぐために最も高い IOPS フロアを必要とするデータベース トランザクション ログボリュームに使用します。
最高レベル（データベース共有データ用）	システム定義	16,384	32,768	2,000	1	複数のホストからアクセスされる共有データベースボリュームで、高いスループットと安定したレイテンシが求められる場合に使用します。

Name	Type	想定IOPS/TB	ピークIOPS/TB	絶対最小IOPS	想定される遅延時間（ミリ秒）	サマリ
最高レベルのパフォーマンス	システム定義	6,144	12,288	1,000	1	高バーストIOPSと予測可能な低レイテンシを必要とするHPC、AI/ML、および分析ワークロードに使用します。
Performance	システム定義	2,048	4,096	500	2	仮想化アプリケーションやエンタープライズアプリケーションで、極端なIOPS要求なしに信頼性の高いパフォーマンスが求められる場合に使用します。
Value	システム定義	128	512	75	17	ホームディレクトリ、ファイル共有、アーカイブなど、コスト重視のワークロードに使用します。

容量ポリシー

Name	Type	スペースリザベーション	自動成長モード	階層化ポリシー	ボリュームタイプ（NAS）	サマリ
default	システム定義	システムデフォルト	システムデフォルト	なし	システムデフォルト	プラットフォームのデフォルトの容量動作で問題ない一般的なワークロードに使用してください。
本番	システム定義	システムデフォルト	拡張	なし	システムデフォルト	容量不足による障害を防ぐために自動的に拡張する必要のある本番環境のワークロードに使用します。

セキュリティポリシー

Name	Type	暗号化	ランサムウェア対策	FIPS	サマリ
default	システム定義	any	any	any	プラットフォームのデフォルトのセキュリティ動作が許容されるワークロードに使用してください。
ランサムウェア対策	システム定義	any	on	any	機密情報またはビジネス クリティカルなデータを含むワークロードで、アクティブなランサムウェア対策が必要な場合に使用します。
本番	システム定義	有効	any	any	コンプライアンス遵守のために暗号化が必須となる本番環境のワークロードに使用します。

データ保護ポリシー

Name	Type	1時間ごとのスナップショット	日々のスナップショット	週間スナップショット	月次スナップショット	サマリ
default	システム定義	6	2	2	0	長期的なデータ保持のオーバーヘッドを必要とせず、短期的な復旧ポイントを必要とする標準的なワークロードに使用します。
3month-hourly	システム定義	23	6	4	3	規制対象またはビジネス クリティカルなワークロードで、日中の詳細な復旧ポイントと3か月分の履歴データ保持が必要な場合に使用します。

NetApp Console ローカル展開で事前定義されたストレージクラスポリシーを確認する

NetApp Console のローカル展開には、4つのポリシータイプすべてにわたるシステム定義ポリシーが含まれます。ストレージクラスを作成またはカスタマイズする際に、ワークロードの要件に最適なポリシーを特定するために、このリファレンスを参照してください。

パフォーマンスポリシー

最高レベルのパフォーマンス
: 高バーストIOPSと予測可能な低レイテンシを必要とするHPC、AI/ML、および分析ワークロードに使用します。

最高レベル（データベース データ用）
: 持続的に高いIOPSとミリ秒以下のレイテンシを必要とするトランザクショナルデータベースのデータボリュームに使用します。

最高レベル（データベース ログ用）
: 書き込みボトルネックを防ぐために最も高い IOPS フロアを必要とするデータベース トランザクション ログボリュームに使用します。

最高レベル（データベース共有データ用）
: 複数のホストからアクセスされる共有データベースボリュームで、高いスループットと安定したレイテンシが求められる場合に使用します。

Performance
: 仮想化アプリケーションやエンタープライズアプリケーションで、極端なIOPS要求なしに信頼性の高いパフォーマンスが求められる場合に使用します。

Value
: ホームディレクトリ、ファイル共有、アーカイブなど、コスト重視のワークロードに使用します。

容量ポリシー

自動拡張容量
: 容量不足による障害を防ぐために自動的に拡張する必要のある本番環境のワークロードに使用します。

セキュリティポリシー

保存時の暗号化
: コンプライアンス遵守のために暗号化が必須となる本番環境のワークロードに使用します。

ランサムウェア対策
: 機密情報またはビジネス クリティカルなデータを含むワークロードで、アクティブなランサムウェア対策が必要な場合に使用します。

標準セキュリティ
: プラットフォームのデフォルトのセキュリティ動作が許容されるワークロードに使用してください。

データ保護ポリシー

default
: 長期的なデータ保持のオーバーヘッドを必要とせず、短期的な復旧ポイントを必要とする標準的なワークロードに使用します。

3month-hourly
: 規制対象またはビジネス クリティカルなワークロードで、日中の詳細な復旧ポイントと3か月分の履歴データ保持が必要な場合に使用します。

30日間の回復期間
: 長期的なデータ保持のオーバーヘッドを必要とせず、短期的な復旧ポイントを必要とする標準的なワークロードに使用します。

90日間の回復
: 規制対象またはビジネス クリティカルなワークロードで、日中の詳細な復旧ポイントと3か月分の履歴データ保持が必要な場合に使用します。

NetApp Console ローカル展開でストレージクラスを作成する

NetApp Console のローカル展開でストレージクラスを作成し、フリート全体でストレージのプロビジョニングと管理方法を標準化します。ストレージクラスとは、パフォーマンス目標、容量動作、セキュリティ要件、データ保護スケジュールなどのストレージクラスポリシーを、単一の名前付き定義にまとめた再利用可能なテンプレートです。

ユーザー（または自動化）がストレージクラスを使用してボリュームまたはLUNをプロビジョニングする場合、NetApp Console のローカル展開では、クラスのポリシーが自動的に適用されます。プロビジョニング後、Console のローカル展開は、ストレージクラスに対するワークロードを継続的に監視してずれを検出し、コンプライアンスを回復するための修復をガイドまたは自動化できます。

開始する前に

- 少なくとも1つのONTAPクラスターを検出して、Console のローカルデプロイメントに配置推奨事項のタ

ーゲットが存在するようにしてください。

- 組織管理者ロール（または、お使いの環境においてストレージクラス管理権限を付与するロール）が付与されていることを確認してください。
- ストレージクラスはポリシーから構成されるため、パフォーマンス、容量、セキュリティ、データ保護など、使用予定のストレージクラスポリシーを作成（または特定）してください。

ストレージクラスを作成する

ストレージクラスを追加するには、組織管理者、フォルダ管理者、またはフリート管理者のいずれかの役割が必要です。

手順

1. 「ストレージ」>「管理」を選択します。
2. 「ストレージクラス」を選択します。
3. *追加*を選択します。
4. 「基本情報」欄に、以下の情報を入力してください。
   - ストレージクラス名：ストレージクラスの一意の名前を入力してください。
   - 概要：（オプション）ストレージクラスの説明を入力してください。
   - 推奨アプリ：（任意）ストレージクラスに推奨されるアプリのリストを入力してください。
5. *ストレージポリシー*で、ストレージクラスに関連付けるポリシーを1つ以上選択します。
6. *追加*を選択します。

既存のストレージクラスをカスタマイズする

既存のストレージクラスをカスタマイズするには、組織管理者、フォルダ管理者、またはフリート管理者のいずれかの役割が必要です。

手順

1. 「ストレージ」>「管理」を選択します。
2. 「ストレージクラス」を選択します。
3. カスタマイズするストレージクラスで、**...** を選択し、複製 を選択します。
4. *基本情報*で、必要に応じて以下の情報を更新してください。
   - ストレージクラス名：ストレージクラスの一意の名前を入力してください。
   - 概要：（オプション）ストレージクラスの説明を入力してください。
   - 推奨アプリ：（任意）ストレージクラスに推奨されるアプリのリストを入力してください。
5. *ストレージポリシー*で、ストレージクラスに関連付けるポリシーを1つ以上選択します。
6. *追加*を選択します。

ユーザー定義ストレージクラスを編集する

ユーザー定義のストレージクラスを編集するには、組織管理者、フォルダ管理者、またはフリート管理者のいずれかの役割が必要です。

手順

1. 「ストレージ」>「管理」を選択します。
2. 「ストレージクラス」を選択します。
3. 編集するストレージクラスについて、*...*を選択し、次に*編集*を選択します。
4. 「基本情報」の項目で、必要に応じて以下の内容を編集してください。
   - ストレージクラス名：ストレージクラスの一意の名前を入力してください。
   - 概要：（オプション）ストレージクラスの説明を入力してください。
   - 推奨アプリ：（任意）ストレージクラスに推奨されるアプリのリストを入力してください。
5. *ストレージポリシー*で、ストレージクラスに関連付けるポリシーを1つ以上選択します。
6. *Edit*を選択します。

ユーザー定義ストレージクラスを削除する

ユーザー定義のストレージクラスを削除するには、組織管理者、フォルダ管理者、またはフリート管理者のいずれかの役割が必要です。

手順

1. 「ストレージ」>「管理」を選択します。
2. 「ストレージクラス」を選択します。
3. 削除するストレージクラスに対して、... を選択し、次に 削除 を選択します。
4. *Delete*を選択します。

   この操作は元に戻せないことにご注意ください。現在使用中のストレージクラスを削除した場合、そのクラスでプロビジョニングされたボリュームまたはLUNは引き続き動作しますが、削除されたクラスとは関連付けられなくなります。

NetApp Console ローカル展開でのストレージ プロビジョニング

NetApp Console のローカルデプロイメントでボリュームと LUN をプロビジョニングして、ワークロードに必要なストレージリソースを利用可能にします。プロビジョニングの際に、オプションでストレージクラスを選択して、定義済みのストレージポリシーと組織標準を適用できます。

必要なアクセスロール

スーパー管理者、組織管理者、フォルダまたはフリート管理者、またはストレージ管理者。"アクセスロールについて"。

ボリュームをプロビジョニングする

手順

1. 「ストレージ」>「管理」を選択します。
2. 「Fleets」を選択します。

3. プロビジョニングを行うフリートを選択してください。
4. *追加*を選択します。
5. メニューから「Volume」を選択してください。
6. ボリュームの詳細：
   a. ボリューム名を入力してください。
   b. 容量を入力してください（必要に応じて単位を選択してください）。
   c. （オプション）ストレージクラスポリシーを適用するストレージクラスを選択します。選択しない場合、ボリュームはストレージクラスポリシーなしでプロビジョニングされます。
7. *システム詳細*の下：
   a. 選択したフリートに適したシステムの中から、1つのシステムを選択してください。
   b. Storage VMを選択します。
8. 「ホスト（NAS）の詳細」で、ホストがボリュームにアクセスする方法を選択します：
   a. NFSによるエクスポート（エクスポートポリシーによって、どのNFSホストがボリュームにアクセスできるかを制御できます）
   b. SMB/CIFS による共有
9. *追加*を選択します。

LUNをプロビジョニングする

手順

1. 「ストレージ」>「管理」を選択します。
2. 「Fleets」を選択します。
3. プロビジョニングを行うフリートを選択してください。
4. *追加*を選択します。
5. メニューから「LUNs」を選択してください。
6. **LUN** ストレージの詳細：
   a. 接頭辞名を入力してください。
   b. そのプレフィックスを使用して作成するLUNの数を入力してください。
   c. LUNごとの容量を入力してください（必要に応じて単位を選択してください）。
   d. （オプション）ストレージクラスポリシーを適用するストレージクラスを選択します。選択しない場合、LUN はストレージクラスポリシーなしでプロビジョニングされます。
7. *システム詳細*の下：
   a. システムを選択してください（プロンプトが表示された場合）。
   b. Storage VMを選択します。
8. *ホスト（SAN）の詳細*で、ホストがボリュームにアクセスする方法を選択します。
   a. ホストオペレーティングシステム（Windows または Linux など）を選択して、LUN のアライメントとブロックサイズに関する推奨デフォルト値を設定します。

b. ホストマッピンググループを選択して、どのイニシエータが LUN にアクセスできるかを制御します。

9. *追加*を選択します。

ストレージの状態を監視する

NetApp Console ローカル展開におけるストレージ監視

NetApp Console のローカル展開機能を使用すると、ダッシュボード、アラート、詳細な分析、および修復機能によって、複数のストレージ群を監視できます。これにより、ワークロードに影響が出る前に問題を特定して解決できます。

ダッシュボードを使用してフリート全体の健全性を監視する

まずはダッシュボードを使って、ストレージの状態とパフォーマンスを素早く把握します。ホームページでは一目でわかる指標を確認し、ダッシュボードテーブルを開いて定義済みダッシュボードやカスタムダッシュボードを表示し、さらに詳細な情報が必要な場合はアラート、調査、および修復のセクションに移動します。

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開でダッシュボードを最新の状態に保つ"
- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"

パフォーマンスの問題を調査する

ワークロードアナライザーを使用して、個々のボリュームのパフォーマンス問題を調査します。レイテンシ、スループット、IOPS、および構成変更を相関させることで、根本原因を特定できます。

- "NetApp Console ローカル展開ワークロードアナライザーについて"
- "NetApp Console ローカル展開でボリュームの高レイテンシを調査する"
- "NetApp Console ローカル展開におけるボリュームの高スループット需要を調査する"
- "NetApp Console ローカル展開における Workload Analyzer のメトリックについて"

アラートと通知を設定する

注意が必要なストレージの状態について、適切な担当者が通知を受け取れるように、アラートポリシーと通知チャネルを設定してください。例えば、容量に関する警告はストレージチームに、保護に関するアラートはそれに対応できるバックアップ管理者にルーティングします。

"NetApp Console ローカル展開での通知とアラートポリシーの設定"."NetApp Console ローカル展開でストレージアラートを表示する".

問題を解決する

問題が検出されたら、NetApp Console のローカル展開から直接修復します：

- 自動修復 — NetApp Console のローカル展開では、事前定義されたルールに基づいて修正措置が自動的に適用されます。

- ガイド付き修復 — 各操作を完全に制御しながら、段階的な推奨事項に従って問題を解決します。

ダッシュボードで監視する

NetApp Console ローカル展開でホームページのメトリクスを表示する

ホームページのダッシュボードを、ストレージの状態とパフォーマンスを監視するためのデフォルトの開始点として NetApp Console ローカル展開で使用してください。フリートの状態、アラート、セキュリティ、容量使用率、レイテンシ、スループット、IOPS に関する概要メトリクスを提供します。

ホーム画面のダッシュボードは、閲覧権限のあるフリートとシステムのみが表示されるように自動的に設定されます。役割に応じた監視を行うために、ホームページにカスタムダッシュボードを追加することもできます。

カードは、階層的なトリアージワークフローとして使用してください。リスクのホットスポットを見つけるには、まず「フリートの健全性」と「アラート」を確認してください。影響を受けるリソースを特定するには、「システム健全性ステータス」と「推奨される修復策」を使用してください。根本原因を調査するには、「容量使用量」、「レイテンシ」、「スループット」、および「IOPS」を使用してください。

フリートの健全性

Fleet health カードには、上位5つのフリートの概要ステータスサマリーが表示されます。システム数、使用容量、セキュリティコンプライアンス、および重大なアラートが含まれます。このカードを使用して、どのフリートに早急な対応が必要かを特定してください。選択したフリート専用のダッシュボードを表示するには、フリート名を選択してください。

推奨される改善策

「推奨される対策」カードには、発生している問題と推奨される対策が記載されています。このカードは、容量負荷、オフラインリソース、および保護関連のリスクに基づいて、修復措置の優先順位を決定します。

アラート

*アラート*カードには、選択した期間内のアラートの件数が要約され、重要度別にグループ化されます。このカードを使用して、現在のインシデント発生状況を把握し、重大、警告、または情報アラートの最近の変更点を確認してください。

セキュリティ

「セキュリティ」カードには、システムコンプライアンスやランサムウェア関連の制御など、コンプライアンスと保護に関する指標がまとめられています。このビューを使用して、リソース全体のセキュリティ傾向を監視します。

容量使用量

「容量使用状況」カードには、選択したフリートまたはシステム全体の予測および過去の使用傾向が表示されます。このカードを使用して成長パターンを把握し、追加容量の計画を立ててください。

[レイテンシ]

レイテンシー カードは、選択したシステム全体における応答時間の推移を追跡します。この傾向を利用し

て、発生しつつあるパフォーマンス遅延を検出し、リソース間の相対的なレイテンシを比較します。

スループット

*スループット*カードには、選択したシステムのデータ転送速度の推移が表示されます。このカードを使用して、ワークロードの強度を把握し、スループット需要の変化を監視します。

[IOPS]

*IOPS*カードは、時間の経過に伴う入出力動作率を示します。このカードを使用して、システム間のアクティビティレベルを比較し、持続的または断続的なI/O需要を特定します。

ダッシュボードカード（例：メトリックカード）

下部の*ダッシュボード*領域には、選択したプロダクションスコープの平均レイテンシなど、ユーザーが選択したカスタムダッシュボードを含めることができます。これらのカードは、チーム別、作業量別、または目標別に、集中的なモニタリングを行う際に使用します。

システムの状態

*システム健全性ステータス*カードには、個々のシステムとその現在の健全性状態が表示されます。このカードを使用すると、異常なシステムを迅速に特定し、ステータスの変化をアラートやパフォーマンスシグナルと関連付けることができます。

関連情報

- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"

カスタムダッシュボードを使用する

NetApp Console ローカル展開におけるカスタムダッシュボードについて

カスタムダッシュボードを NetApp Console のローカル展開で使用することで、特定のチーム、フリート、ワークロード、および運用目標に特化した監視ビューを作成できます。カスタムダッシュボードは、ホームページのダッシュボードを補完し、広範囲にわたる常時利用可能な監視機能に対象を絞った可視性を追加します。

ダッシュボードの種類がどのように連携して機能するか

ホームページダッシュボード

容量、アラート、パフォーマンス容量、ライセンス、データ保護ステータスを監視するための、すぐに使用できるモニタリングパネル。ビューは事前に設定されており、自動的に更新されます。"NetApp Console ローカル展開でホームページのメトリクスを表示する"。

カスタムダッシュボード

役割に応じた監視ビューは、事前定義されたカードから構築され、選択可能なスコープ、メトリクス、対象リソース、および時間枠が含まれます。

両方を併用してください：* ホームページから始めて、毎日のベースラインモニタリングを行います。* チーム、フリート、ワークロード、または運用上の疑問点ごとに、カスタムダッシュボードを使用して集中的な調

査を行います。

ホーム画面には、一度に1つのカスタムダッシュボードを追加できます。

カスタムダッシュボードを理解する

カスタムダッシュボードとは、保存したカードのコレクションをグリッド上に配置するものです。各カードは、指標とグラフの種類が事前に定義されたカードテンプレートに基づいています。カードを追加する際には、スコープ、対象オブジェクト、集計方法、および時間枠を設定します。

カスタムダッシュボードとカードは、お客様専用のものです。各カードには、閲覧権限が付与されているストレージリソースのデータのみが表示されます。

監視の優先順位が変わった場合、ホームページからカスタムダッシュボードを削除し、別のダッシュボードを追加することができます。

重要なことを監視する

カードテンプレートは指標の種類ごとに整理されているため、ダッシュボードを特定の業務領域に絞り込むことができます。例えば、容量カードを使用して、予想よりも速いペースで増加しているボリュームを監視したり、アラートカードを使用して、ビジー状態のクラスタで繰り返し発生する障害を追跡したりできます：

Performance

フリート全体、システム、SVM、ボリューム、LUNにおけるレイテンシ、IOPS、スループット、利用率、およびパフォーマンス容量。

Capacity

フリート、システム、SVM、ボリューム、LUN、およびローカルティア全体における使用容量、空き容量、使用容量率、およびスナップショット容量。

Health

健全性状態、劣化または重大なオブジェクトの数、ディスク障害、ネットワークインターフェースエラー、およびホットオブジェクト。

アラート

重大なアラートの件数、深刻度別のアラート、影響範囲別のアラート、最近のアラート、および時間の経過に伴うアラートの傾向。

定義済みのカードと指標の完全なカタログについては、"NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"を参照してください。

リソースタイプ

カードのスコープは、ONTAP ストレージ階層の任意のレベル（フリート、クラスタ、システム（ノード）、SVM、ボリューム、LUN、およびローカルティア（アグリゲート））に設定できます。利用可能なリソースの種類は、選択したカードテンプレートによって異なります。

プランのダッシュボードビュー

ワークロードのパフォーマンスのトリアージ、容量計画、健全性リスク検出、アラートの優先順位付けなど、ストレージ管理の目標に合わせてカスタムダッシュボードを整理します。

関連情報

- "NetApp Console ローカル展開でのダッシュボードの使用を開始する"
- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"

NetApp Console ローカル展開でのダッシュボードの使用を開始する

NetApp Console のローカル展開では、以下のワークフローに従って、広範囲のビューから焦点を絞ったビューまで監視します。ホームページのダッシュボードを確認し、定義済みのダッシュボードを確認し、カスタムダッシュボードを作成し、ダッシュボードを最新の状態に保ちます。

必要なアクセスロール

すべての役割。ダッシュボードには、閲覧権限のあるリソースのみが表示されます。利用可能なリソースの一覧に目的のリソースが表示されない場合、そのリソースを表示する権限がありません。


ホームページで基本的な正常性を確認する

ホームページのダッシュボードを使用して、組織レベルのキャパシティ、アラート、パフォーマンス、およびデータ保護ステータスを確認します。

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開におけるストレージ監視について"


その他の定義済みダッシュボードを確認する

*ストレージ > ダッシュボード*を開いて、役割に応じた追加のビューを示す定義済みダッシュボードを確認してください。

- "NetApp Console ローカル展開でダッシュボードを管理する"


集中的な監視のためのカスタムダッシュボードを作成する

特定のリソース、指標、および期間を対象としたビューが必要な場合は、カスタムダッシュボードを作成します。

- "カスタムダッシュボードを作成する"
- "NetApp Console ローカル展開でダッシュボードカードをカスタマイズする"


ダッシュボードを常に最新の状態に保つ

優先順位の変更に応じて、カスタムダッシュボードを編集、複製、または削除することで、ダッシュボードを更新します。

- "NetApp Console ローカル展開でダッシュボードを管理する"

- "NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"

関連情報

- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "NetApp Console ローカル展開でホームページのメトリクスを表示する"

NetApp Console ローカル展開で目標を監視するためのダッシュボードを作成する

NetApp Console のローカル展開でカスタムダッシュボードを作成し、カードを追加して、日常業務用の監視ビューを保存します。

すぐに使える組織レベルの監視機能だけが必要な場合は、あらかじめ定義されたホームページのダッシュボードから始めてください。役割に応じたビュー、リソースレベルのターゲティング、またはカスタマイズされたカードレイアウトが必要な場合は、カスタムダッシュボードを作成してください。

コンソールローカル展開ダッシュボードガイドライン

- ダッシュボードを作成したユーザーのみが閲覧できます。コンソールのホーム画面にダッシュボードを追加した場合でも、他のユーザーと共有することはできません。
- 閲覧権限のあるリソースのみ閲覧できます。利用可能なリソースの一覧に目的のリソースが表示されない場合、そのリソースを表示する権限がありません。
- 開始する前に、ダッシュボードで追跡したい指標の種類とリソースを特定してください。"NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"

監視目標に合わせたダッシュボードを作成する

フリートの健全性、パフォーマンスのホットスポット、アラートの傾向など、お客様の役割にとって重要な指標を一か所で監視する必要がある場合は、ダッシュボードを作成してください。

手順

1. 「ストレージ」>「ダッシュボード」を選択します。
2. 「ダッシュボードを追加」を選択します。

   コンソールでのローカル展開では、デフォルト名で説明のない新しいダッシュボードが作成されます。
3. 「カードを追加」を選択します。
4. カードの リソースタイプ （フリート、システム、ボリュームなど）を選択し、利用可能なリソースのリストからリソースを選択します。
5. 「次へ」を選択して、指標とカードの種類の選択に進みます。
6. 表示する指標を選択してください。利用可能なメトリックは、メトリックタイプ：パフォーマンス、キャパシティ、ヘルス、または*アラート*でフィルタリングするか、名前で特定のメトリックを検索できます。利用可能な指標は、選択したリソースの種類によって異なります。

   "利用可能な指標について説明します。"
7. ダッシュボードに含めるカードを選択し、*次へ*を選択します。

   一度に選択できるカードは1枚のみです。カードのプレビューには、選択したメトリックとリソースタイプのリアルタイムデータが表示されます。

8. カードに名前を付けてください。ダッシュボード内では、名前は一意である必要があります。
9. カードのプレビューを確認し、カード名と説明を入力してから、*追加*を選択してください。
10. 追加のカードについても、これらの手順を繰り返してください。
11. 鉛筆アイコンを選択して、ダッシュボードの名前と説明を編集し、その目的を記述します。
12. 「カードを追加」ボタンの右側にあるアクションメニューを選択し、「ダッシュボードを保存」を選択します。

    保存されたダッシュボードは、*ストレージ > ダッシュボード*からアクセスできます。
13. 必要に応じて、アクションメニューから「ホームページに追加」を選択して、このダッシュボードをホームページに追加できます。ダッシュボードがホームページに追加されました。作成したカスタムダッシュボードは、お客様のみが閲覧できます。他者と共有されることはありません。

関連情報

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "NetApp Console ローカル展開でダッシュボードカードをカスタマイズする"
- "NetApp Console ローカル展開でダッシュボードを管理する"

NetApp Console ローカル展開でカードをカスタマイズする

NetApp Console のローカル展開では、SLA リスク、容量負荷、繰り返し発生するアラートノイズなど、オペレーターが最も重要なシグナルに集中できるよう、ダッシュボードカードをカスタマイズできます。このトピックを参考に、チームが行う必要のある業務上の意思決定に合わせてダッシュボードの表示を設定してください。

開始する前に

- カードを配置したいダッシュボードを作成または開きます。
- 利用可能なテンプレートと指標を"NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"で確認します。

既存のダッシュボードを改良しながらカードを追加する

既存のダッシュボードを改良する際に、特定の運用上の疑問に答えるカードをすばやく追加する必要がある場合は、このオプションを使用してください。

手順

1. カードを追加したいダッシュボードを開きます。
2. 「カードを追加」を選択します。
3. カードの リソースタイプ （フリート、システム、ボリュームなど）を選択し、利用可能なリソースのリストからリソースを選択します。
4. 「次へ」を選択して、指標とカードの種類の選択に進みます。
5. 表示する指標を選択してください。利用可能なメトリックは、メトリックタイプ：パフォーマンス、キャ

パシティ、ヘルス、または*アラート*でフィルタリングするか、名前で特定のメトリックを検索できます。利用可能な指標は、選択したリソースの種類によって異なります。

"利用可能な指標について説明します。"

6. ダッシュボードに含めるカードを選択し、*次へ*を選択します。

   一度に選択できるカードは1枚のみです。カードのプレビューには、選択したメトリックとリソースタイプのリアルタイムデータが表示されます。

7. カードに名前を付けてください。ダッシュボード内では、名前は一意である必要があります。
8. カードのプレビューを確認し、カード名と説明を入力してから、*追加*を選択してください。
9. 追加のカードについても、これらの手順を繰り返してください。
10. ダッシュボードを保存します。

関連情報

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "カスタムダッシュボードを作成する"
- "カスタムダッシュボードを管理する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードカードとメトリクスについて"

定義済みダッシュボードとカスタムダッシュボードカードのリファレンス（ **NetApp Console** ローカル展開）

NetApp Console のローカル展開では、事前定義されたダッシュボードとカスタムダッシュボードカードテンプレートにより、ONTAP のパフォーマンス、キャパシティ、健全性、およびアラート運用の監視範囲が提供されます。

事前定義済みダッシュボード

以下の定義済みダッシュボードは、すぐに利用可能です。

Name	説明
ボリューム	ボリュームパフォーマンス、容量、QoS、FabricPool、成長率、および予測指標。
満杯になるまでの時間	ONTAP クラスター、ボリューム、およびアグリゲートの容量がいっぱいになるまでの時間予測。
セキュリティ	セキュリティコンプライアンス、暗号化、自律型ランサムウェア対策、および認証の概要。
SVM	ONTAP SVM のパフォーマンス、容量、ボリューム、LIF、プロトコル（CIFS、FCP、iSCSI、NFS、NVMe/FC）、QoS、およびレイテンシのヒートマップ監視。
電力	ノード、シェルフ、およびアグリゲートに対するONTAPクラスタの消費電力、温度、ファン速度の監視。

Name	説明
ノード	ONTAPノードのパフォーマンス、CPU、ネットワーク、およびバックエンドの監視。
Network	ネットワークパフォーマンス指標には、イーサネット、FibreChannel、NVMe/FC、リンクアグリゲーショングループ、およびルートが含まれます。
LUN	ONTAP LUN のパフォーマンス、容量、および効率の監視。
Health	ONTAPクラスターの状態監視には、エラー、警告、EMSアラート、HAの問題、ノード/ディスク/シェルフの状態、ボリューム、ライセンス、ネットワークポートなどが含まれます。
アグリゲート	ONTAP アグリゲートの容量、効率比率、および成長率のモニタリング。

ダッシュボードレベルの時間枠と集計

選択可能な時間帯は、30分、1時間、24時間、48時間、7日間、30日間です。集計オプションはテンプレートによって異なり、フリート全体のロールアップや上位N件の結果表示などのビューが含まれます。時間枠と集計はダッシュボードレベルで設定され、ダッシュボード内のすべてのカードに適用されます。

ダッシュボードカードのテンプレートと指標

カードは、カスタムダッシュボードの構成要素です。各カードは、メトリックとチャートタイプを含む事前定義されたテンプレートを使用し、そのビューを特定の ONTAP オブジェクトと監視目標にマッピングします。

カードテンプレートはあらかじめ定義されており、ユーザーが作成することはできません。

ストレージ操作メトリック指標（概要）

メトリックの種類は、パフォーマンスのボトルネック、容量の逼迫、健全性リスク、アラート量など、一般的なストレージ管理の結果に対応しています。

メトリックタイプ	サポートされている指標	ストレージ管理者のユースケース	詳細テンプレート
Performance	平均レイテンシ、ピークレイテンシ、IOPS、スループット（MB/s）、利用率、パフォーマンス容量	ボトルネック、持続的なプレッシャー、およびパフォーマンスの余裕を特定する	テンプレートに移動
Capacity	使用容量、空き容量、使用容量（%）、スナップショット使用容量	成長を追跡し、空き容量の少ない領域を特定し、スナップショットの影響を監視します。	テンプレートに移動
Health	健康状態、劣化/重大オブジェクト、ディスク障害、ネットワークインターフェースエラー、ホットオブジェクト（レイテンシ別）	健全性の低下を検出し、運用上のトリアージを優先する	テンプレートに移動
アラート	アラート（重大）、深刻度別アラート、影響範囲別アラート、最近のアラート、アラートの傾向	発生中のインシデントを監視し、アラートの量を時系列で傾向分析する	テンプレートに移動

サポート対象ONTAPオブジェクト階層（リソースタイプ）

カードデータは、フリートレベルの可視性からオブジェクトレベルのトラブルシューティングまで、複数のONTAP オブジェクトレベルで表現できます。

*リソースタイプ*の設定は、以下のリソースレベルの1つ以上にマッピングされます。

- 艦隊
- クラスタ
- システム（ノード）
- SVM
- Volume
- LUN
- ローカル階層（アグリゲート）

利用可能なリソースレベルは、選択したテンプレートとメトリックによって異なります。

運用分析用のグラフの種類

グラフの種類は、トレンド、比較、分布、およびポイントインタイム値をどれだけ早く解釈できるかに影響します。

グラフの種類	最適な用途
折れ線グラフ	レイテンシ、IOPS、スループット、利用率、アラートの推移など、時系列のトレンド。
棒グラフ	深刻度別または影響範囲別のアラートなど、カテゴリ別の比較と分布。
パイかドーナツ	使用容量の割合など、比例配分。
テーブル	使用容量、健全性ステータス、最近のアラートなど、詳細な複数列のデータ。
単一の数値（統計）	重要なアラート件数や故障したディスクなど、主要な値を一目で把握できます。

ワークロードトリアージのためのパフォーマンステンプレート

パフォーマンステンプレートは、ワークロードの負荷を示すレイテンシ、スループット、および利用率のシグナルに焦点を当てています。

テンプレート	グラフの種類	説明
平均レイテンシ	ライン	選択した時間枠における、選択したターゲット全体の平均レイテンシ。
ピークレイテンシ	ライン	選択した時間枠内で、選択したターゲット全体で観測された最大レイテンシ。
[IOPS]	ライン	選択されたターゲット全体における1秒あたりの入出力操作の合計。
スループット（MB/秒）	ライン	選択されたターゲット全体におけるデータスループットの合計。

テンプレート	グラフの種類	説明
利用率	ライン	選択されたターゲット全体における平均CPUまたはディスク使用率。
パフォーマンス容量	テーブル	現在の利用状況と最適ポイントを比較するヘッドルーム分析。

成長と余裕のためのキャパシティテンプレート

キャパシティテンプレートは、成長計画とリスク検出をサポートするために、消費済みスペースと利用可能スペースに焦点を当てています。

テンプレート	グラフの種類	説明
使用容量	テーブル	選択されたターゲット全体で使用された容量の合計。
空き容量	テーブル	選択された対象全体における、空き容量または利用可能な容量の合計。
使用容量（%）	パイかドーナツ	選択されたターゲット全体における、使用量と総量の平均比率。
スナップショット容量使用状況	テーブル	選択されたターゲット全体で消費されたスナップショット領域の合計。

リスク検出のためのヘルステンプレート

ヘルステンプレートは、運用上のトリアージを支援するために、オブジェクトの状態と障害指標に焦点を当てています。

テンプレート	グラフの種類	説明
ヘルスステータス	テーブル	選択された各対象オブジェクトの最新の健全性状態。
劣化/重大なオブジェクト	単一の番号	健康状態が良好でないオブジェクトの数。
障害ディスク	単一の番号	選択されたシステムにおける、故障したディスクの合計数。
ネットワークインターフェースエラー	パイかドーナツ	選択されたターゲット全体におけるネットワークインターフェースのエラーカウンタの合計。
レイテンシの高いホットオブジェクト	テーブル	リソースは、ピークレイテンシの降順でランク付けされています。

インシデントの優先順位付けのためのアラートテンプレート

アラートテンプレートは、監視と優先順位付けを支援するために、インシデントの発生件数、深刻度、および影響範囲に焦点を当てています。

テンプレート	グラフの種類	説明
アラート（重大）	単一の番号	指定時間枠内における重大度（クリティカル）アラートの件数。
重要度別アラート	バー	アラートは重要度レベル別にグループ化されています。

テンプレート	グラフの種類	説明
影響エリア別のアラート	バー	容量、パフォーマンス、セキュリティなど、影響範囲別にグループ化されたアラート。
最近のアラート	テーブル	最新のアラートを、時間順に降順で表示します。
アラートトレンド	ライン	選択した時間帯における、時間帯ごとのアラート件数。

関連情報

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "カスタムダッシュボードを作成する"
- "NetApp Console ローカル展開でダッシュボードカードをカスタマイズする"
- "カスタムダッシュボードを管理する"

カスタムダッシュボードを管理する

NetApp Console ローカル展開でダッシュボードを管理する

NetApp Console のローカルデプロイメントでカスタムダッシュボードを管理し、ビューと運用を整合させます。チーム、フリート、優先順位の変更に応じて、ダッシュボードの編集、複製、削除を行うことができます。

このタスクは、ストレージ > *ダッシュボード*にあるカスタムダッシュボードにのみ適用されます。事前定義されたホームページのダッシュボードは、同じ方法では編集できません。

ダッシュボードを表示する

カスタムダッシュボードと定義済みダッシュボードを表示して、開きたい、編集したい、複製したい、または削除したいダッシュボードを見つけてください。

定義済みのダッシュボードを複製して、編集可能なカスタムバージョンを作成できます。

手順

1. 「ストレージ」>「ダッシュボード」を選択します。
2. ダッシュボードの表を確認し、開きたいダッシュボードを探してください。
3. ダッシュボード名を選択して開き、その指標を確認してください。
4. 必要に応じて、利用可能な操作を使用してカスタムダッシュボードを編集、複製、または削除します。

優先順位が変わったらダッシュボードを更新する

業務上の優先順位が変わり、表示するカードや指標を調整する必要がある場合は、ダッシュボードを編集してください。

手順

1. 「ストレージ」>「ダッシュボード」を選択します。
2. 編集したいダッシュボードを開きます。
3. ダッシュボード上の既存のカードを変更するには、カードのアクションメニューから「編集」を選択します。
4. *カードを追加*を選択して、ダッシュボードに新しいカードを追加します。

   "NetApp Console ローカル展開でカードをカスタマイズする".

5. ダッシュボードを保存するには、*変更を保存*を選択してください。
   - アクションメニューから「新しいダッシュボードとして保存」を選択することで、変更内容を新しいダッシュボードとして保存することもできます。このオプションは、他のチームやフリート向けに元のダッシュボードを維持しつつ、現在の監視ニーズに合わせて新しいバージョンを作成したい場合に便利です。
   - アクションメニューから「変更を破棄」を選択することで、変更内容を破棄することもできます。このオプションは、ダッシュボードを最後に保存したバージョンに戻したい場合に便利です。

別のリソースまたはフリートにカスタムダッシュボードを再利用する

実績のあるレイアウトを別のチーム、フリート、または監視シナリオで再利用したい場合は、ダッシュボードを複製することで、ゼロから再構築する必要がなくなります。

定義済みのダッシュボードを複製して、編集可能なカスタムバージョンを作成できます。

手順

1. 「ストレージ」>「ダッシュボード」を選択します。
2. 複製したいダッシュボードに対して、アクションメニューから*複製*を選択します。

   コンソールのローカル展開では、元のダッシュボードのすべてのカードを含むコピーが作成されます。

3. 複製したダッシュボードの名前と説明を入力してください。
4. 先ほど作成した複製ダッシュボードを選択してください。新しい監視シナリオに合わせて、指標、リソース、カードの種類を変更してください。

   "NetApp Console ローカル展開でカードをカスタマイズする".

使用しなくなったダッシュボードを削除する

現在の運用をサポートしなくなったダッシュボードを削除し、ダッシュボードリストをアクティブなユースケースに集中させておきます。

手順

1. 「ストレージ」>「ダッシュボード」を選択します。
2. 削除するダッシュボードで、*削除*を選択します。
3. 削除を確認します。

関連情報

- "NetApp Console ローカル展開でホームページのメトリクスを表示する"
- "NetApp Console ローカル展開でのダッシュボードの使用を開始する"
- "NetApp Console ローカル展開におけるカスタムダッシュボードについて"
- "カスタムダッシュボードを作成する"
- "NetApp Console ローカル展開でダッシュボードカードをカスタマイズする"

NetApp Console ローカル展開でインベントリを使用してフリートを監視する

NetApp Console のローカル展開では、インベントリを使用してフリートの状態を監視し、環境全体のストレージリソースを調査します。インベントリ機能は、容量、セキュリティ、パフォーマンスに関するビューを提供し、問題の特定、リソース使用状況の把握、管理対象ストレージシステムの追跡に役立ちます。

インベントリは、主に情報収集と診断のための作業スペースです。インベントリからは、フリート全体のシステム、ボリューム、その他のストレージオブジェクトを確認したり、ストレージリソースのプロビジョニングなどの一般的な操作を実行したりできます。高度なストレージ管理操作については、NetApp Console のローカル展開により、System Manager にリダイレクトされます。

アクセスインベントリ

Console のローカル展開では、以下を含む複数の場所から **Inventory** にアクセスできます：

- ホームページ
- フリート概要ページ
- フリートヘルスカードと関連するインベントリビュー

Inventory にアクセスする場所によって、表示されるスコープは組織レベルまたはフリートレベルになります。

在庫ビュー

*インベントリ*は、ストレージ環境のさまざまな側面を分析するのに役立つ複数のビューを提供します。

Capacity
: ストレージの使用状況を表示し、ストレージリソースを消費しているシステム、ボリューム、その他のストレージオブジェクトを特定します。

セキュリティ
: 管理対象ストレージリソース全体におけるセキュリティ関連情報およびコンプライアンス状況を確認します。

Performance
: パフォーマンス関連の指標を分析し、さらなる調査が必要となる可能性のあるリソースを特定します。

表示される情報は、選択したビューとオブジェクトの種類によって異なります。

ストレージリソースを調査する

*インベントリ*を使用して次の操作を行います。

- フリートの健全性を監視する
- ストレージ容量の使用状況を確認する
- 管理対象ストレージシステムの追跡
- 容量を消費するボリュームやその他のオブジェクトを特定する
- 潜在的なセキュリティ問題またはパフォーマンス問題を調査する
- 管理上の対応が必要なリソースを特定する

*インベントリ*は、お客様の環境の概要レベルの可視性から、特定のストレージリソースのより詳細な調査へと移行するのに役立ちます。

ストレージリソースをプロビジョニングする

インベントリには、ボリュームやLUNなどのストレージリソースをプロビジョニングできるワークフローが含まれています。

リソースをプロビジョニングする際には、既存のマネージドストレージシステムを選択し、ワークロードに必要な構成設定を指定します。

インベントリとアラート

アラートは、お客様の環境内の特定のストレージオブジェクトおよび条件に基づいて生成されます。

アラートを選択すると、Console のローカル展開によって、追加の調査や管理アクションのために System Manager に誘導される場合があります。*インベントリ*は、ストレージ環境と管理対象リソースの全体的な状態をより広範に可視化することで、アラートを補完します。

高度な管理タスク

*インベントリ*は、対応が必要なリソースを特定するのに役立ちますが、高度なストレージ管理操作の一部は System Manager で実行されます。

例としては以下のようなものがあります：

- 高度なワークロード管理
- リソースの再配置と最適化タスク
- 詳細なシステム管理作業

問題の特定と調査には「Inventory」を使用し、より高度な管理機能が必要な場合は「System Manager」を使用してください。

アラートを修正する

NetApp Console ローカル展開のアラートについて

NetApp Console のローカル展開により、オンプレミス ONTAP クラスターおよび NetApp Backup and Recovery 操作における健全性の問題を特定するアラートが生成されます。

コンソールのローカル展開は、ONTAPクラスターとバックアップおよびリカバリ操作からのアラートを単一のビューに統合します。アラートページには、ダッシュボード、アラート一覧、およびシステムビューが含まれており、組織全体のアラートを確認したり、特定のフリートやシステムに絞り込んでアラートを表示したりできます。各アラートは、影響を受けるシステム、その重大度、および影響範囲を示します。

コンソールのローカル展開でアラートを使用して、次のことを行います。

- 容量、接続性、データ保護、パフォーマンス、およびセキュリティの問題を検出します。
- アラートの優先順位を、重要度と影響範囲に基づいて決定します。
- システムマネージャーまたはワークロードアナライザーでアラートを開き、ページにガイド付きまたは自動の Fix-It アクションが表示されたら、それを実行します。
- 指定されたアクセス権限を持つユーザーにメールで通知を送信するか、Webhookを介してアラートデータを外部システムに送信します。
- アラートリストをCSVファイルにエクスポートして、オフラインで分析します。

アラートの重大度と影響範囲

各アラートには、重大度と影響範囲が含まれています。

- *重大度*は緊急度を示し、高い順から低い順に、Critical、Major、Minor、Warning、Info となります。
- *影響範囲*は、容量、接続性、データ保護、パフォーマンス、セキュリティといった影響を受ける領域を示します。

アラートの発生源と範囲

- *ONTAPアラート*は、NetApp Consoleのローカル展開によって検出されたオンプレミスクラスター上のONTAP イベント管理システム（EMS）から発信されます。"ONTAP EMSと利用可能なアラートの詳細をご確認ください。"
- *NetApp Backup and Recovery alerts*は、Backup and Recoveryの操作から発生します。"NetApp Backup and Recovery のアラートの詳細をご確認ください。"
- 閲覧できるフリートは、お客様の権限によって決まります。表示範囲を組織全体、特定のフリート、または個々のシステムに限定します。「システムの状態」タブにはシステムごとの状態が表示され、「アラート」タブには選択した範囲の現在のアラート一覧が表示されます。
- CSVエクスポートには、現在のスコープ、検索テキスト、およびフィルターが反映されます。

アラート通知ルール

どの警告が通知を生成するか、そして誰が通知を受け取るかを決定する通知ルールを作成します。通知ルールには、以下の特徴があります：

- サービス（ONTAP 管理や Backup and Recovery など）、重大度、影響範囲、および対象システムに関するアラートと照合します。

- メール配信の場合、指定されたアクセス権限を持つユーザーに通知を送信します。Webhook配信の場合、アラートデータは設定されたエンドポイントに送信されます。そのデータへのアクセスは、NetApp Consoleのローカル展開ではなく、受信側のアプリケーションによって制御されます。
- これは特定のシステムに適用されるものであり、フリート全体には適用されません。
- 計画メンテナンス期間中は、予期されるアラートを抑制するために、この機能をミュートすることができます。

コンソールのローカル展開には、インストール直後に有効になるデフォルトの通知ルールが含まれています。デフォルトのルールでは、すべてのサービスとシステムを監視してクリティカル重大度のアラートを検出し、コンソール通知センターにのみ通知を送信します。メールやWebhookによる配信は、設定するまで構成されません。このルールを表示および調整したり、環境に合わせてカスタムルールを作成したりできます。

情報レベルのアラートはアラートページに表示されますが、情報レベルの重大度を含むルールを明示的に作成しない限り、通知によって配信されません。

関連情報

- "アラートを監視し、調査する"
- "アラート通知ルールの作成と管理"
- "NetApp Console ローカル展開における ONTAP アラートについて"

NetApp Console ローカル展開でアラートを監視および調査する

NetApp Console のローカルデプロイメントでアラートを監視・調査し、ストレージの健全性を維持して障害を最小限に抑えます。

組織全体または特定のフリート全体のアクティブなアラートを表示し、深刻度と影響範囲に基づいて優先順位を付け、根本原因を調査することで、問題がエスカレートする前に解決できます。アラートに推奨されるアクションや「Fix It」オプションが含まれている場合、調査から直接修復作業に移行できます。

必須アクセスロール

Federation admin と Federation viewer を除くすべてのロール。Federation admin または Federation viewer ロールを持つユーザーは、アラートを表示できません。"アクセスロールについて"。

ONTAP アラートの場合、アラートページから直接 System Manager や Workload Analyzer などのツールにアクセスして、問題の調査と解決を行うことができます。

外部への報告のために、アラートリストをCSVファイルにエクスポートしてオフラインで分析することができます。

また、通知ルールを設定して、メールまたはWebhookでアラートを受信することもできます。"アラート通知の設定方法について説明します"。

利用可能なアラート

NetApp Console のローカル展開は、ONTAP および NetApp Backup and Recovery のアラートをサポートします。

- "NetApp Console ローカル展開における ONTAP アラートについて"

- "NetApp Backup and Recovery のアラートの詳細をご確認ください。"

アラートダッシュボードを表示する

アラートダッシュボードを使用すると、選択した範囲における現在のアラートアクティビティをすばやく確認できます。ダッシュボードには、発生中のアラートが深刻度と影響範囲別にまとめられており、過去24時間のアラート分布を示すグラフも含まれているため、傾向を素早く把握できます。

ダッシュボードをフィルタリングして、重要なアラートや特定の影響範囲に関するアラートに絞り込むことができます。

手順

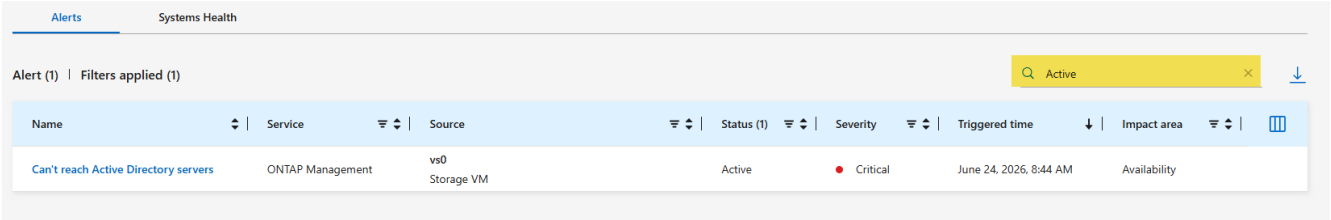
1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. 表示する必要のあるアラートに応じてダッシュボードをフィルタリングします。フィルタリング対象には以下が含まれます：
   - 深刻度（重大、警告、または情報）
   - 影響領域別にグループ化されたクリティカルアラート
   - 影響範囲（セキュリティ、保護、可用性、パフォーマンス、容量、または構成）

すべてのアラートを表示

選択したスコープのアクティブなアラートの全リストを表示するには、「アラート」タブを使用します。リストは現在の組織またはフリートのスコープを反映して更新され、名前や説明で特定のアラートを検索できます。

手順

1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. 選択したスコープの有効なアラートの全リストを表示するには、*アラート*タブを選択してください。
4. 必要に応じて、名前または説明で特定の警告をリスト内から検索できます。



システム別にアラートを表示する

フリートまたは組織内の特定のシステムに関するアラートを表示できます。

手順

1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. **Systems health** タブを選択すると、選択した範囲内のシステムに関連付けられているアラートの概要が表示されます。
4. 該当システムの行にある「アラートを表示」を選択すると、そのシステムに関連付けられているアクティブなアラートの全リストが表示されます。

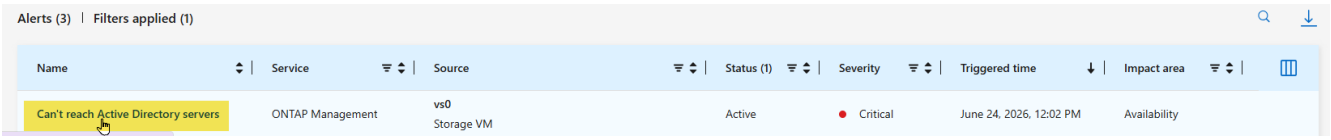
アラートを調査する

アラートを調査することで、何がアラートを引き起こしたのか、誰が通知を受け取ったのかを確認できます。

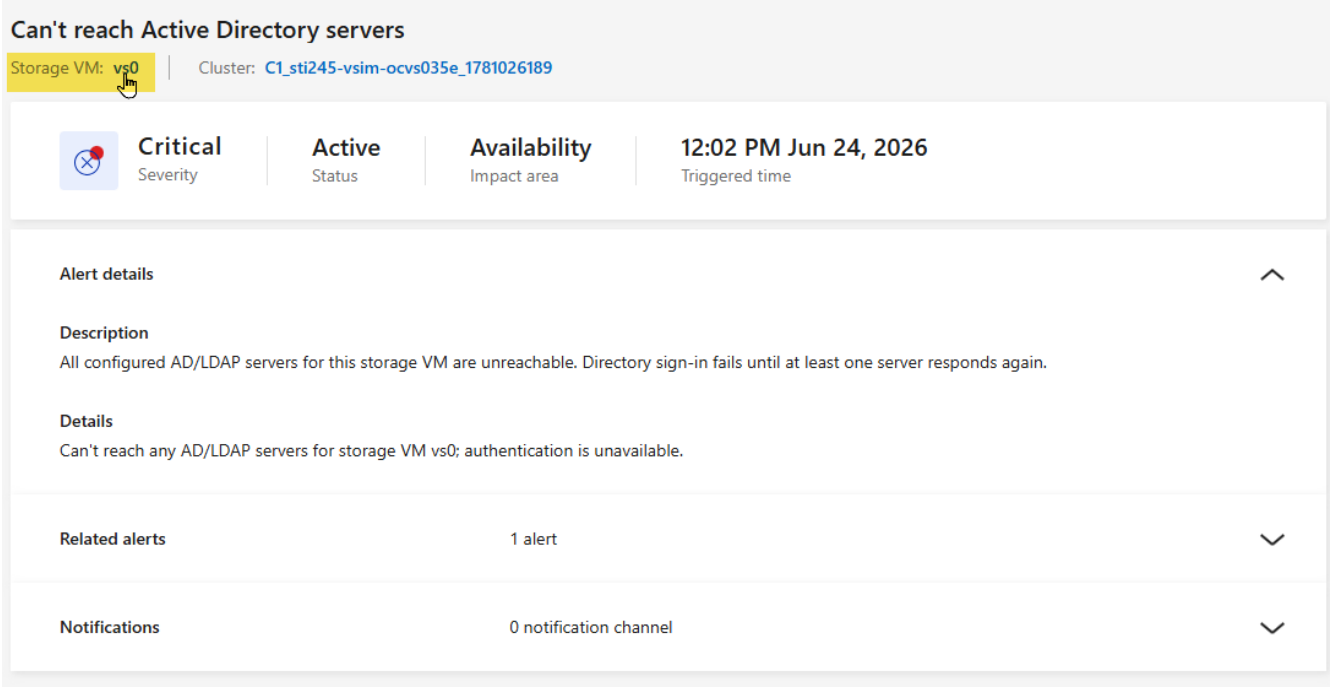
ONTAP アラートを調査する際、アラートを生成したシステムの System Manager インターフェースに直接アクセスして、詳細情報を確認したり、必要な措置を講じたりすることもできます。

手順

1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. どちらのタブでも、調査したいアラートの名前を選択すると、その詳細が表示されます。



4. 該当する場合は、アラートを生成したシステムの System Manager インターフェイスを開くために、VM またはクラスタ名を選択してください。



アラートを修復する

アラートに推奨されるアクションまたは「Fix It」オプションが含まれている場合は、アラートの詳細画面から離れることなく、それらを使用して調査から修復へと移行してください。

手順

1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. 対処したいアラートを選択してください。
4. アラートの詳細を確認し、推奨される対処方法、または利用可能な場合は「Fix It」オプションを選択してください。
5. ガイドの手順に従って修復措置を適用し、その後アラートの詳細画面に戻ってアラートの状態を確認してください。

その措置によって問題が解決した場合、その範囲におけるアラートはアクティブとして表示されなくなります。アラートが引き続き有効な場合は、アラートの詳細を再度確認し、調査を継続してください。

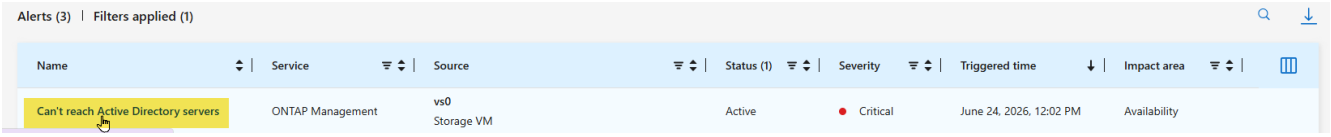
アラートを分析する

ワークロードアナライザーでONTAPアラートを分析し、何がトリガーとなったかを把握できます。

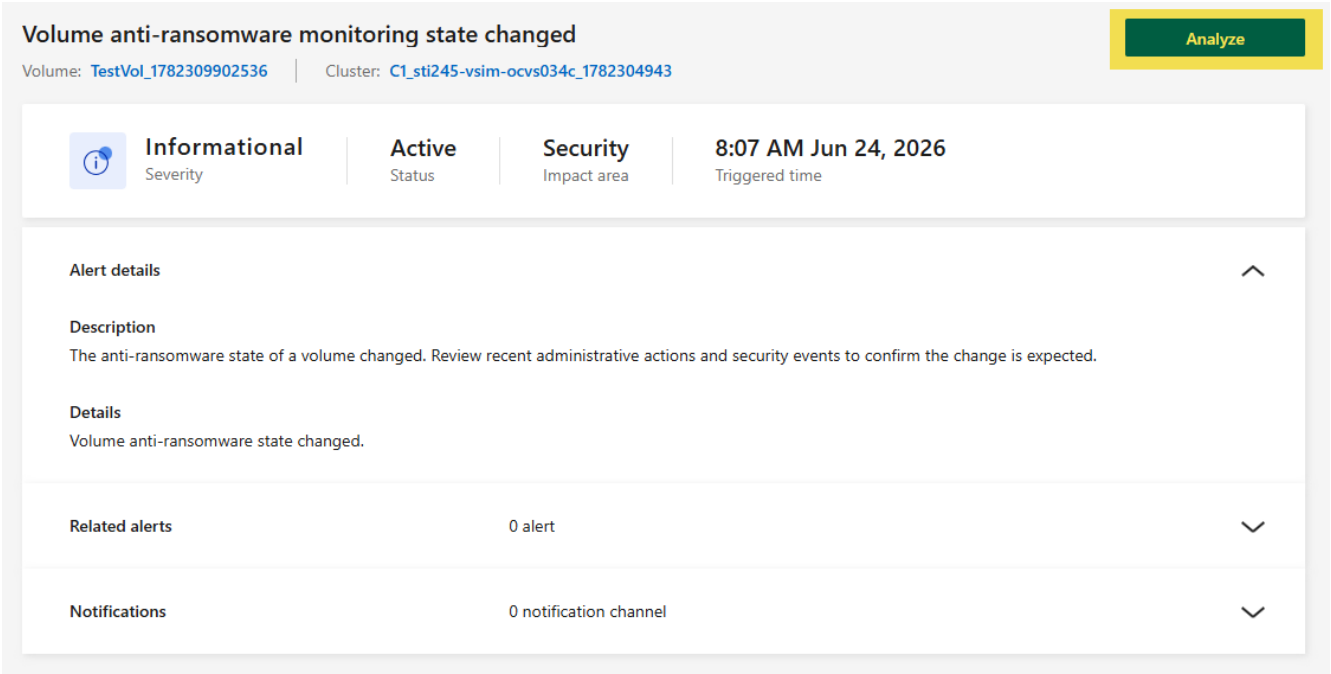
ONTAP アラートを調査する際、アラートを生成したシステムの System Manager インターフェースに直接アクセスして、詳細情報を確認したり、必要な措置を講じたりすることもできます。

手順

1. **Health > Alerts > Overview** を選択します。
2. スコープセレクターから、以下のいずれかを選択してください。
   - すべて（デフォルト）を選択すると、アクセス権のあるすべてのフリートのアラートが表示されます。
   - 特定のフリートに関するアラートのみを表示する
3. 選択した範囲のアクティブなアラートの全リストを表示するには、**Systems health** タブを選択してください。
4. どちらのタブでも、調査したいアラートの名前を選択すると、その詳細が表示されます。



5. 該当する場合は、*分析*を選択して、アラートを生成したシステムのワークロードアナライザーインターフェイスを開きます。



6. アラートがトリガーされた期間をカバーする時間範囲を入力し、*分析*を選択して分析結果を表示します。"ワークロードアナライザーについて説明します。"

アラートを**CSV**ファイルにエクスポート

NetApp Console のローカルデプロイメントのアラートリストを CSV ファイルにエクスポートして、オフラインでの分析やレポート作成に使用します。エクスポートされるデータには、現在のスコープ（組織またはフリート）、検索テキスト、およびフィルターが反映されます。

手順

1. **Health > Alerts** を選択し、アラート タブを選択します。
2. 対象範囲（組織またはフリート）を設定し、エクスポートに含めるフィルターや検索テキストを適用します。

3. アラートリストをCSVファイルにエクスポートするには、ダウンロードアイコンを選択してください。

NetApp Console ローカル展開でアラートの通知ルールを設定する

NetApp Console ローカル展開で通知ルールを設定して、どのアラートが通知を発生させるか、誰が通知を受け取るか、そしてどのように通知が配信されるかを制御します。

必要なアクセスロール

スーパー管理者、組織管理者、ストレージ管理者、運用サポートアナリスト、または NetApp Backup and Recovery の管理者ロールのいずれか。"アクセスロールについて"。

通知ルールを使用することで、適切なアラートを環境に合ったチャネルを通じて適切な担当者にルーティングし、お客様に関係のないアラートによるノイズを削減できます。通知ルールはアラートページを補完するものです。アラートワークフローでアラートを調査または修復した後、ルールを使用して、今後同様のアラートがどのように配信されるかを制御できます。

通知ルールは、サービス、重要度、影響範囲など、お客様が定義した条件に基づいてアラートを照合し、選択したチャネルを通じて通知を配信します。Console のローカル展開には、表示および調整可能なデフォルトの通知ルールが含まれており、独自のカスタムルールを作成することもできます。メンテナンス期間などの計画されたイベント中に通知を一時的に抑制するために、ルールをミュートすることもできます。

- "ONTAP EMSと利用可能なアラートの詳細をご確認ください。"

開始する前に

- メールで通知を配信するには、組織管理者がコンソールのローカル展開環境でメールサーバーを設定する必要があります。外部システムに通知を送信するには、組織の管理者がWebhookを設定する必要があります。手順については、"通知配信の設定"を参照してください。
- コンソールのローカル展開通知センターはデフォルトで通知を表示するため、コンソール内通知に関する追加の設定は不要です。

通知ルールを表示する

通知ルールページは、組織に適用されるすべてのルールを確認および管理するための中心的な場所です。各ルールにはその主要な属性が表示されるため、アラートの動作を迅速に評価し、調整することができます。

手順

1. 左側のナビゲーションから、**Health > Alerts** を選択します。
2. 「通知設定」を選択します。
3. リストに記載されているルールを確認してください。各ルールには、その有効状態、名前、監視対象のサービスと重要度レベル、通知を受信する権限を持つ役割、有効な配信チャネル、最終更新日時、およびスケジュールされたミュート期間が表示されます。
4. 特定のルールを見つけるには、フィルターと検索コントロールを使用して、アクティブ状態、サービス、重要度、役割、チャネル、またはミュート状態によって絞り込みます。

通知ルールを作成する

通知ルールを作成して、通知をトリガーする条件と、その通知の配信方法を定義します。

フリートに対して通知ルールを設定することはできません。特定のシステムに対してのみ設定できます。多数のシステムが存在する大規模な環境では、システムごとにルールを重複させるのではなく、重要度に基づいてより広範なルールを作成することを検討してください。たとえば、すべてのシステムを対象とする1つの Critical ルールを包括的なルールとして設定し、異なるルーティングや受信者が必要なシステムには、追加のターゲットルールを設定するといった方法です。

全システムにおける重大アラートの通知ルール例

発生源がどのシステムであっても、重大なアラートを見逃さないようにしたいとします。ストレージ管理者向けに、すべての重大なアラートを Console Notification Center にルーティングする包括的なルールを作成できます。

この例では、以下の設定でルールを作成します。

- サービス：すべて
- 重大度：Critical
- **IAM**ロール：ストレージ管理者
- **System**：（すべてのシステムに適用する場合は、この欄を空欄にしてください）
- 配信方法：Console Notification Center

このルールが適用されると、ストレージ管理者は、すべてのシステムにおける重大なアラートが発生するたびに、Console に通知を受け取ります。このルールは基準となるものであり、より具体的なルールを追加することで補完できます。

ストレージ管理者の容量アラートを対象とした通知ルールの例

ストレージ管理者が特定の運用システムにおける重大な容量問題に即座に対応する必要があるものの、重要度の低いアラートが受信トレイに大量に届くのは避けたいとします。特定のシステムで重大な容量アラートが発生した場合にのみ、ストレージ管理者にメールを送信するターゲットルールを作成できます。

この例では、以下の設定でルールを作成します。

- サービス：ONTAP管理
- 重大度：Critical
- 影響範囲：容量
- **IAM**ロール：ストレージ管理者
- システム：<system_name>
- 配信方法：メール

このルールが適用されている場合、Console のローカル展開では、容量に関する重大なアラートが発生した際に、指定されたシステムのすべてのストレージ管理者に電子メールが送信されます。警告や情報提供など、重要度の低いアラートはメールを生成しないため、チームは緊急の対応が必要な問題に集中できます。

手順

1. 左側のナビゲーションから、**Health > Alerts** を選択します。
2. 「通知設定」を選択し、次に「ルールの追加」を選択します。

3. ルールが一致する条件を定義します。
    - ルール名：簡潔で分かりやすい名前を入力してください。この項目は必須です。
    - ルールの説明：必要に応じて、ルールの目的に関する追加情報を入力してください。
    - サービス：ルールが適用される ONTAP またはプラットフォームサービスを1つ以上選択してください。
    - 役割：ルールがトリガーされたときに通知を受け取るためにユーザーが持つ必要があるアクセス役割を選択します。
    - 重要度レベル：ルールが監視する重要度レベル（Critical、Warning、Error、Information など）を選択します。
    - 影響範囲：容量やパフォーマンスなど、一致させる運用領域を選択します。
    - アラート名：ルールをトリガーする特定のアラートの種類を選択します。
    - システム：ルールを適用するシステムコンテキストを選択します。
4. 通知の配信チャネルを選択します：
    - メール：選択した役割を持つユーザーにアラートメールを送信します。設定済みのメールサーバーが必要です。
    - **Webhook**：アラートデータを外部システムに送信します。設定済みのWebhook連携を選択する必要があります。
    - **Console Notification Center**：選択されたロールを持つユーザーに対するリアルタイムアラートを表示します。
5. 必要に応じて、メンテナンス期間などの計画された期間中にこのルールからの通知を抑制するには、*通知をミュート*スケジュールを設定し、ミュート期間を繰り返す場合は繰り返しを選択してください。ルールごとに複数のミュート期間を追加できるため、週ごとのパッチ適用などの定期的なメンテナンスサイクルに便利です。
6. 「作成」を選択します。

通知ルールを有効または無効にする

個々の通知ルールを有効または無効にすることで、どの条件で通知が発生するかを制御できます。環境に関係のないルールを無効にしてノイズを減らし、ルールを有効にして通知を再び受信できるようにしてください。

手順

1. 左側のナビゲーションから、**Health > Alerts** を選択します。
2. 「通知設定」を選択します。
3. 変更するルールを見つけます。
4. ルールの **Active** スイッチをオンまたはオフに切り替えます。変更はすぐに有効になります。

通知ルールをミュートする

通知ルールをミュートすることで、ルールを無効にすることなく、メンテナンス期間などの計画されたイベント中にアラートの配信を抑制できます。ミュート期間中もアラートは Alerts ページに引き続き表示されます。メール、webhook、およびコンソール内通知のみが抑制されます。ミュート期間が終了すると、通知は自動的に再開されます。

1つのルールに複数のミュート期間を追加し、それぞれをスケジュールに基づいて繰り返し実行するように設

定できます。

ミュートウィンドウの例

- 一時的なメンテナンス期間：土曜日の夜にストレージシステムのファームウェアアップグレードを実行する場合、その期間中に発生するはずのアラートを抑制したいとします。土曜日の午後10：00から日曜日の午前2：00までをミュート期間として設定し、繰り返しは設定しません。期間が終了すると、通知は自動的に再開されます。
- 毎週の定期的なパッチ適用時間：チームは毎週日曜日の午前0時から午前4時までシステムにパッチを適用します。週単位の繰り返し設定でミュート期間を追加すると、手動で操作することなく、毎週自動的に通知が抑制されます。別のシステムに異なる時間帯の独自のパッチ適用スケジュールがある場合は、独自の開始時刻と繰り返し設定を持つ2つ目のミュート期間を同じルールに追加してください。

手順

1. 左側のナビゲーションから、**Health > Alerts** を選択します。
2. 「通知ルール」を選択します。
3. ルール一覧から、ミュートしたいルールを見つけ、そのルールのアクションメニューを選択します。
4. *Edit*を選択します。
5. 「通知をミュート」セクションで、ミュート期間の開始日時と終了日時を設定します。
6. 必要に応じて、スケジュールに基づいてウィンドウを繰り返すための繰り返し設定を選択します。
7. ミュートウィンドウを追加するには、*ミュートウィンドウを追加*を選択し、前の手順を繰り返してください。
8. 「保存」を選択します。

通知ルールを削除する

不要になった通知ルールは削除してください。ルールを削除すると完全に削除されるため、復元することはできません。

手順

1. 左側のナビゲーションから、**Health > Alerts** を選択します。
2. 「通知設定」を選択します。
3. ルール一覧から削除したいルールを見つけ、そのルールのアクションメニューを選択します。
4. アクションメニューから*削除*を選択してください。

関連情報

- "通知配信の設定"
- "コンソールアラートについて"
- "アラートを表示する"

NetApp Console ローカル展開におけるストレージクラスのドリフトの修正

NetApp Console のローカル展開で、ドリフト関連のアラートを検出し、ドリフトの検出結果を分析し、ストレージクラスの意図と一致しなくなったワークロードを修復しま

す。

必須の役割

Storage Admin

権限が付与されているフリート内のワークロードのみを表示および修復できます。

ドリフトを修正する

ワークロードがストレージクラスの意図と一致しなくなった場合、NetApp Console のローカル展開でアラートが発生します。アラートを使用してドリフトを分析し、推奨される修復措置を適用してください。

アラートから直接、いくつかの対策を適用できます。その他の問題については、ワークロード構成を更新するか、別のストレージクラスを割り当ててコンプライアンスを回復してください。修復ワークフローでは、変更を適用する前に想定される影響が表示されます。

手順

1. 「Storage」>「Storage classes」を選択してください。

   ストレージクラスの変動の概要は、「ストレージクラス別の変動」エリアに表示されます。完全なリストは表に表示されます。

2. 「Drifts」列で、該当するストレージクラスの「View」を選択します。

   「アラート > 概要」ページを開くと、フィルターが適用された状態になります。

3. アラートを選択すると、アラートの詳細ページが開きます。
4. 「分析」を選択します。
5. **Workload analyzer** で結果を確認してください。

   設定のずれが判明した場合は、意図した設定と実際の設定を比較して、何が変更されたかを判断してください。

6. 「Fix it」など、推奨される修復措置を選択してください。
7. 提案された変更内容を確認し、是正措置を適用してください。
8. 「Storage」＞「Storage classes」に戻り、ワークロードがずれた状態として表示されなくなったことを確認してください。

   コンプライアンス評価には、最近の設定変更を反映させるのに数分かかる場合があります。ワークロードが依然として「ずれ」と表示される場合は、アラートの詳細ページに戻り、*分析*を選択して残りの検出結果を確認してください。

関連情報

- "NetApp Console ローカル展開におけるストレージクラスのドリフトとコンプライアンスについて"
- "ストレージアラートについて"
- "アラートを表示する"

NetApp Console ローカル展開におけるアラート修復アクション

このリファレンスを使用して、NetApp Console ローカル展開の **Fix it** で利用可能な修復アクションを確認してください。各アクションについて、表にはそのアクションの内容と関連するアラートが記載されています。実行する前に、確認ダイアログに表示される操作の詳細を確認してください。

是正措置

是正措置	アラート名	アラートの説明	影響範囲	修復の概要
自動ボリューム増加を有効にする	ボリュームがいっぱいです	ボリュームの空き容量が少なくなっており、ほぼ満杯の状態です。	Capacity	容量不足のリスクを軽減するため、ボリュームのサイズを（設定された上限まで）自動的に拡張します。
ボリュームのサイズを変更する	ボリュームがいっぱいです	ボリュームの空き容量が少なくなっており、ほぼ満杯の状態です。	Capacity	ボリュームのサイズを拡大して、すぐに空き容量を増やします。
ボリュームをオンラインにする	ボリュームはオフライン	ボリュームはオフラインで、データを提供していません。	使用の可否	オフライン ボリュームをオンラインにして、データの提供を再開できるようにします。
アグリゲートをオンラインにする	オフライン アグリゲート	アグリゲートがオンラインではないため、そこにホストされているボリュームが利用できない場合があります。	使用の可否	オフライン アグリゲートをオンラインにして、ホストしているボリュームへのアクセスを復元します。
LUNをオンライン化	LUNオフライン	LUNがオフラインのため、ホストからのアクセスはできません。	使用の可否	オフラインになっているLUNをオンラインに戻し、ホストがアクセスとI/Oを再開できるようにします。
ボリュームの制限を解除	ボリュームは制限状態	ボリュームは制限状態にあり、通常の入出力処理ができない可能性があります。	使用の可否	制限付きボリュームをオンライン状態に戻し、クライアントが再びアクセスできるようにします。
NVMeネームスペースをオンラインにする	NVMe名前空間がオフラインです	NVMeネームスペースがオフラインのため、ホストからのアクセスはできません。	使用の可否	オフラインになっているNVMeネームスペースをオンラインにして、ホストへのアクセスを復元します。
クラスター間**LIF**を起動する	クラスター間LIFダウン	クラスター間LIFがダウンしており、クラスター間の通信に影響が出ている可能性があります。	接続	レプリケーションに使用されるクラスター間の接続を復元するために、クラスター間 LIF を起動します。

是正措置	アラート名	アラートの説明	影響範囲	修復の概要
MetroCluster AUSO の再有効化	MetroCluster 自動計画外スイッチオーバーが無効になっています	このクラスターでは、自動的な計画外切り替えは無効になっています。	使用の可否	自動計画外スイッチオーバー（AUSO）を再度有効にして、MetroCluster保護機能が意図どおりに機能するようにします。
サービスプロセッサネットワークの設定	サービスプロセッサが構成されていません	サービスプロセッサ（SP）ネットワークが設定されていません。	管理性	Service Processor （SP）のネットワーク設定を構成して、アウトオブバンド管理アクセスを有効にします。
未割り当てディスクを割り当てる	未割り当てのディスクが検出されました	割り当てられていないディスクが存在し、利用可能な容量が未使用である可能性があります。ディスクをノードに割り当てて、ストレージとして使用できるようにします。	使用の可否	現在割り当てられていないディスクをノードに割り当て、ストレージとして使用できるようにします。
ルートボリュームスペース回復	ノードルートボリュームの空き容量が少ない	ノードのルートボリュームの空き容量が少なく、システムの正常な動作に影響を与える可能性があります。	システム ヘルス	ノードのルートボリューム上の最大のスナップショットまたは最大のコアダンプファイルを削除することで、空き容量を確保します。削除は元に戻せません。

パフォーマンスの問題を調査する

NetApp Console ローカル展開ワークロードアナライザーについて

NetApp Console ローカル展開のワークロードアナライザーを使用して、単一ボリュームの経時的な動作を表示します。ボリューム自体、アラート、またはインベントリから、パフォーマンスの低下、容量の傾向、およびリソースの競合の問題を調査できます。

ワークロードアナライザーが根本原因を特定する方法

ワークロードアナライザーを使用して、単一のボリュームから6つのセクションにわたるメトリクスを相関させることで、根本原因を迅速に特定できます。ボリュームと時間範囲を選択すると、イベント、パフォーマンス、容量を同じウィンドウ内でまとめて表示できます。このビューは、アプリケーションの問題の原因がストレージにある可能性が高いのか、それともネットワークなどの別のレイヤーが問題を引き起こしているのかを判断するのに役立ちます。

アナライザーは、どのボリュームが影響を受けているかが既にわかっている場合に最も役立ちます。アラートまたはボリュームインベントリから開くと、Console のローカル展開ではボリュームが選択された状態でアナライザーが開くため、分析ウィンドウとグラフに集中できます。

この分析ツールは一度に1つのボリュームしか追跡しないため、複数のボリュームを比較するのではなく、特定の問題を調査するために使用してください。

この評価の一環として、キャパシティのセクションを確認してください。ONTAPシステムが85%以上使用されている場合、高い使用率自体がパフォーマンスの問題を引き起こす可能性があり、そのため、利用可能な容量が少ないことが、パフォーマンスチャートだけでは説明できない遅延の原因となる可能性があります。

根本原因を特定したら、アナライザーから直接対応することができます。自動化オプションが利用可能な場合、Console のローカル展開では、ガイド付き手順またはワンクリック修復による Fix-It の推奨事項が提供されます。

LUNのワークロードチャートはボリュームのチャートほど詳細な情報を提供しないため、LUNを分析する際には表示される統計情報が少なくなります。

アクセスワークロードアナライザー

ワークロードアナライザーを開く方法はいくつかあります：

- 「Health」メニューから「Workload Analyzer」を選択し、「Volume」フィールドで調査対象のボリュームを検索して選択します。
- ストレージ > フリート > インベントリ ページから、分析するボリュームに移動し、アクションメニューから 分析 を選択します。
- *アラート > 概要*ページから、調査するボリュームのアラートを選択し、アラートの詳細から*分析*を選択します。

LUNも分析できますが、ボリュームに比べて表示される統計情報は少なくなります。

レイテンシ、スループット、ストレージ容量を分析する

以下の6つのセクションを使用して、ボリュームを調査します。

ボリューム選択

調査するボリュームと時間範囲を選択すると、すべてのグラフとイベントが同じワークロードと分析ウィンドウに合わせて表示されます。

イベントタイムライン

分析期間中に、選択したボリュームの現在および過去の構成変更、警告アラート、および重大アラートを表示します。このセクションを使用して、「何が変わったか」とパフォーマンスまたはキャパシティ挙動の変化との相関関係を分析してください。

レイテンシ分析

ボリュームの遅延を、合計として、または遅延センター（ネットワーク、データ処理、集計操作、クラスタ インターコネクト、その他）別に分類して経時的に表示します。ボリュームが QoS ポリシーを使用している場合、アナライザーはポリシーの最大および最小レイテンシ制限を基準線として表示するため、ワークロードがスロットリングしきい値にどれだけ近いかを確認できます。予測を切り替えることで、レイテンシが警告または危険しきい値に向かっているかどうかを予測できます。

スループット分析

IOPS と MB/s の経時変化を、オプションで読み取り / 書き込み / その他の内訳とともに表示します。ボリュームが QoS ポリシーを使用している場合、アナライザーは IOPS とスループット制限線を表示します。予測を切り替えることで、需要が QoS 制限に向かっているかどうかを予測できます。

リソース使用率

分析期間中に、ボリュームを処理するノードとアグリゲートのビジー状態を確認します。アナライザーは、値を積み重ねるのではなく、各リソースを独立した線としてプロットするため、特定のノードまたはアグリゲートが競合の原因となっているかどうかを特定できます。予測を切り替えることで、いずれかのリソースが高使用率のしきい値に向かう傾向があるかどうかを予測できます。

容量分析

ボリューム内の物理的なスペースと使用可能なスペースが、時間の経過とともにどのように変化したかを確認できます。カーソルを合わせると、重複排除、圧縮、コンパクションによる節約効果を含むストレージ効率の内訳が表示されます。予測を切り替えることで、ボリュームが警告または重大な容量しきい値に達する時期を予測できます。スナップショットビューに切り替えると、スナップショット領域が設定されたスナップショット予約領域に対してどのように使用されているかを確認できます。

容量とパフォーマンスの傾向を予測する

各分析セクションにある予測トグルを使用して、チャートのタイムラインを現在時刻以降に延長し、観測された傾向に基づいて将来の値を予測します。点線は、予測値と実際のデータを区別する線です。アナライザーは、予測結果から閾値を超える可能性が高いと判断された場合、閾値を超えるまでの推定時間とともに、インサイト メッセージも表示します。

関連情報

"ボリュームの高遅延を調査する"."ボリュームの高スループット要求を調査する"."ボリュームの容量増加を調査する"."NetApp Console ローカル展開における Workload Analyzer のメトリックについて".

NetApp Console ローカル展開でボリュームの高レイテンシを調査する

NetApp Console ローカルデプロイメントのワークロードアナライザーを使用して、ボリュームの応答速度が遅い原因を特定します。

アラートまたはボリュームインベントリからアナライザーを開くと、ボリュームは既に選択されているため、時間範囲とチャートの内訳に集中できます。

アプリケーションのパフォーマンスが低下した場合は、I/Oパスのどの部分が速度低下の原因となっているかを特定してください。レイテンシー分析セクションでは、応答時間を遅延センターごとに分類し、ネットワークの問題、データ処理オーバーヘッド、アグリゲートの競合、およびその他の要因を区別することができます。

手順

1. 以下のいずれかの方法でワークロードアナライザーを開きます。
   - 「Health」メニューから「Workload Analyzer」を選択し、「Volume」フィールドで調査対象のボリュームを検索して選択します。
   - ストレージ > フリート > インベントリ ページから、分析するボリュームに移動し、アクションメニューから 分析 を選択します。
   - *アラート > 概要*ページから、調査対象のボリュームに関連する容量アラートを選択し、アラートの詳細から*分析*を選択します。
2. パフォーマンスの問題が発生していた期間を対象期間として「時間範囲」を設定し、「分析」を選択します。
3. 「イベントタイムライン」セクションを確認して、レイテンシの増加と一致する構成変更とアラートを確認してください。

アナライザーは、構成変更イベント（レンチアイコン）とアラートイベント（警告アイコンと重大アイコン）をレイテンシチャートと同じ時間軸上にプロットするため、変更がパフォーマンス低下に先行していたかどうかを簡単に確認できます。

4. 「レイテンシー」セクションで、「表示」ドロップダウンを開き、「遅延中心による内訳」を選択します。このグラフは、各遅延センターが時間経過に伴う総レイテンシーにどのように寄与しているかを示しています。遅延センターには以下が含まれます：
   - 読み取りレイテンシ
   - 書き込みレイテンシ
   - その他の遅延
5. グラフ上で遅延が最も高いポイントにカーソルを合わせると、各遅延センターの値と、それが全体の遅延に占める割合が表示されます。

   最も遅延が大きい箇所は、通常、競合しているリソースを示しています。共有リソースが需要に追いつけない場合、そのリソースを使用するボリュームはI/O処理でより長い待ち時間が発生します。ワークロードを移動したり、QoS制限を調整したりするなどして、そのリソースへの負荷を軽減し、レイテンシを低減してください。
6. 最も大きな影響を与えている要因を特定し、その値を基に次のステップを決定してください。
   - 読み取りレイテンシが高い場合は、ディスク競合が発生している可能性があります。「リソース使用率」セクションで、アグリゲートのビジー率を確認してください。
   - *書き込みレイテンシ*が大きい場合は、NICの飽和状態、またはクラスタ外のネットワークパスの問題を示している可能性があります。
   - 「その他のレイテンシ」が高い場合は、インライン効率設定がワークロードが許容できる以上のCPUを消費している可能性があります。効率設定またはQoSの調整を検討してください。
   - *クラウドレイテンシ*が高い場合、ワークロードが容量層上のコールドデータに頻繁にアクセスしていることを示している可能性があります。階層化ポリシーの見直しを検討してください。
7. 遅延センターが速度低下を説明していない場合は、「容量分析」セクションを確認してください。ONTAPシステムが 85% を超えて使用されている場合、遅延センターの内訳に関係なく、高い使用率がパフォーマンスの問題を引き起こす可能性があります。
8. 変更イベントの直後にレイテンシが増加した場合は、イベントの詳細と関連するグラフを合わせて、考えられる原因を検証してください。
   - QoSの変更については、レイテンシラインとQoS制限ラインを比較し、スループットチャートを確認して、需要がポリシーの上限に達しているかどうかを確認してください。
   - アグリゲートまたはボリュームの移動については、レイテンシのスパイクを、同じ期間に表示されているノードおよびアグリゲートの利用率の値と比較してください。
   - 階層化ポリシーの変更については、クラウドのレイテンシへの寄与を確認し、変更後にコールドデータへのアクセスが増加したかどうかを判断してください。

終了後の操作

構成または配置の問題が原因で問題が発生し、Console のローカル展開で解決できる場合、ボリュームのアラートに Fix-It オプションが表示されることがあります。

"NetApp Console ローカル展開における Workload Analyzer のメトリックについて".

NetApp Console ローカル展開のワークロードアナライザーを使用して、ボリュームの IOPS とスループット需要を時系列で確認します。

ボリュームのワークロードが予想以上に多くのIOPSまたはスループットを消費している場合は、その需要を引き起こしている要因を特定してください。スループット分析セクションでは、IOPSとMB/sが表示され、オプションで読み取り、書き込み、その他の内訳も表示されるため、どのタイプのI/Oが高い需要を引き起こしているか、またその需要がQoS制限に向かっているかどうかを特定できます。

アラートまたはボリュームインベントリからアナライザーを開くと、ボリュームは既に選択されているため、時間範囲とスループットのグラフに集中できます。

手順

1. 以下のいずれかの方法でワークロードアナライザーを開きます。
   - 「Health」メニューから「Workload Analyzer」を選択し、「Volume」フィールドで調査対象のボリュームを検索して選択します。
   - ストレージ > フリート > インベントリ ページから、分析するボリュームに移動し、アクションメニューから 分析 を選択します。
   - *アラート > 概要*ページから、調査するボリュームのアラートを選択し、アラートの詳細から*分析*を選択します。
2. 「時間範囲」を需要の高い期間に設定し、「分析」を選択してください。
3. 「スループット分析」セクションまでスクロールします。
4. 「表示」ドロップダウンを開き、「内訳（RWO）」を選択します。

   IOPSとMB/sの両方について、グラフは読み取り、書き込み、その他の要素に分けて表示されています。これにより、読み取り中心のアクセスパターン、書き込み中心のアクセスパターン、またはその両方の組み合わせが需要を牽引しているかどうかを判断できます。

5. コンポーネントピッカーを使用して、調査したいメトリクスを有効または無効にします。
   - 読み取り**IOPS***と*書き込み**IOPS** — I/O方向ごとの1秒あたりの操作数
   - 読み取り**MB/s***と*書き込み**MB/s** — I/O方向ごとのスループット（メガバイト/秒）
   - その他の**IOPS***および*その他の**MB/s** — メタデータおよびその他の非データ操作
   - **QoS IOPS**制限*および***QoS MB/s**制限 — ボリュームがQoSポリシーを使用する場合にのみ表示されるポリシーの上限値
   - クラウドスループット — クラウドへの書き込みとクラウドからの読み取りのMB/秒。FabricPoolを通じてクラウドに容量を階層化するワークロードにのみ表示されます。
6. グラフのピークにカーソルを合わせると、その時点における各構成要素の正確な値と割合の内訳が表示されます。

   ホバーツールチップには、各カテゴリの平均I/Oサイズ（スループット÷IOPS）も表示されます。これにより、ワークロードが大規模なシーケンシャルI/Oを実行しているか、小規模なランダムI/Oを実行しているかを確認できます。

7. *予測を表示*を有効にすると、現在のスループット傾向がQoS IOPSまたはMB/sの制限に達するかどうかを予測できます。

予測ラインがQoS制限ラインに近づいている場合、ONTAPは近いうちにワークロードを制限する可能性があります。

8. 内訳を表示せずに総需要を確認したい場合は、**View** ドロップダウンを開き、**Totals** を選択してください。

   合計ビューには、IOPSの行が1つとMB/sの行が1つ表示されるため、全体的な需要の概要を素早く把握するのに役立ちます。

終了後の操作

観察したスループットパターンに基づいて、次に何をすべきかを判断してください。

- 読み取りIOPSが書き込みIOPSに比べて非常に高い場合は、先読み設定やキャッシュによってボリュームへの負荷を軽減できるかどうかを検討してください。
- ワークロードがQoS IOPSまたはMB/sの制限に近づいている、あるいは既に制限に達している場合は、QoS制限行と関連するメトリック定義を使用してスロットリングを確認し、制限を調整する必要があるかどうかを判断してください。
- スループットが高く、かつレイテンシも高い場合は、「リソース使用率」セクションを確認し、基盤となるノードまたはアグリゲートが競合状態にあるかどうかを判断してください。同じ期間におけるスループットのピーク値、レイテンシの急上昇、およびリソース使用率を比較してください。
- 需要が増加している中でアナライザーが容量またはスナップショットの急激な増加を示している場合は、容量とスナップショットの指標を確認して、その増加がボリュームにどのような影響を与える可能性があるかを把握してください。

"ボリュームの高遅延を調査する"."NetApp Console ローカル展開における Workload Analyzer のメトリックについて".

NetApp Console ローカル展開でボリュームの容量増加を調査する

NetApp Console ローカルデプロイメントのワークロードアナライザーを使用して、ボリュームの空き容量が不足している理由を調査します。

ボリュームの容量が不足している場合や、スナップショットコピーが予想以上に多くの容量を消費している場合は、容量とスナップショットの傾向を時系列で確認してください。容量分析セクションでは、物理的なスペースと利用可能なスペースがどのように変化するか、ストレージ効率による節約効果の内訳、およびボリュームが容量のしきい値に達する時期の予測を示します。

アラートまたはボリュームインベントリからアナライザーを開くと、ボリュームは既に選択されているため、容量の傾向と予測期間に集中できます。

手順

1. 以下のいずれかの方法でワークロードアナライザーを開きます。
   - 「Health」メニューから「Workload Analyzer」を選択し、「Volume」フィールドで調査対象のボリュームを検索して選択します。
   - ストレージ > フリート > インベントリ ページから、分析するボリュームに移動し、アクションメニューから 分析 を選択します。
   - *アラート > 概要*ページから、調査するボリュームのアラートを選択し、アラートの詳細から*分析*を選択します。

2. 「期間」を容量増加期間に合わせて設定し、「分析」を選択してください。
3. 「容量分析」セクションまでスクロールしてください。
4. 「表示」ドロップダウンから「容量ビュー」を選択します。

   このグラフでは、下段の積み重ねられた領域が物理容量を、上段の積み重ねられた領域が使用可能な容量を示しています。これらを合わせるとボリュームの合計サイズになるので、使用可能なスペースがどれほど急速に減少しているかがわかります。

5. グラフ上のポイントにカーソルを合わせると、重複排除、圧縮、コンパクションによる節約効果を含むストレージ効率の内訳と、全体的なストレージ効率比率が表示されます。

   物理的な容量が増加しているにもかかわらず効率比率が低下している場合、新しく書き込まれたデータが既存のデータほど重複排除や圧縮がうまく行われていないことを示している可能性があります。

6. スナップショットの使用状況を調査するには、「View」ドロップダウンから「Snapshot View」を選択します。

   このグラフは、スナップショットリザーブを水平の基準線として、スナップショットの使用容量をその下の領域として示しています。カーソルを合わせると、使用されているスナップショットの容量とそのリザーブに対する割合、スナップショットの総数、および最も古いスナップショットの経過時間が表示されます。

   スナップショットの使用量が予約容量を超えると、スナップショットはボリュームのデータ領域から領域を消費し始め、新しい書き込みに使用できる領域が減少します。

7. ボリュームがクラウドにデータを階層化している場合は、「表示」ドロップダウンから「クラウド階層ビュー」を選択して、ローカルのパフォーマンス階層とクラウドの容量階層の容量を比較します。
8. *予測を表示*を有効にすると、ボリュームが警告または重大な容量しきい値に達する時期を予測できます。

   容量予測には少なくとも10日間の履歴データが必要です。容量が満杯になるまでの残り日数が30日未満になると、アナライザーはストレージがほぼ満杯であると認識します。予測には、違反までの推定時間を示すインサイトメッセージが表示されます。

終了後の操作

観察したキャパシティの傾向に基づいて、次に何をすべきかを決定してください。

- 利用可能な容量が満杯に近づいている場合は、ボリュームサイズを増やす、自動拡張を有効にする、またはボリュームからデータを移動することを検討してください。
- スナップショットの使用容量が予約容量を超えている場合は、スナップショットポリシーと保持ポリシーを見直して容量を解放してください。
- ストレージ効率比が低下している場合は、ワークロードのデータタイプまたはインライン効率設定が節約効果を低下させていないかを確認してください。容量、スナップショット、および効率性指標の詳細については、"NetApp Console ローカル展開における Workload Analyzer のメトリックについて"を使用してください。

ワークロードアナライザーのメトリクス（**NetApp Console** ローカル展開）

NetApp Console のローカル展開では、ワークロードアナライザーが6つのセクションに

わたるメトリックを表示します。各メトリックの説明では、アナライザーがチャート上にメトリックをどのように表示するか、およびそれがボリュームの動作について何を示しているかを説明します。

遅延チャートにおける**QoS**基準線

選択したボリュームが QoS ポリシーを使用している場合、メトリックピッカーで 2 つの追加参照線を使用できます。

基準線	説明
最大 QoS	QoSポリシーによって定義される最大レイテンシの上限。レイテンシ線がこの線に近づくか触れると、ONTAPはワークロードをスロットリングしており、物理リソースではなくQoS制限がレイテンシの主な原因となります。
最小 QoS	QoSポリシーによって定義される、保証された最小遅延レベル。この行は、ワークロードに対して適用される応答時間の下限値を示しています。他のワークロードがスループットを保証するためにQoS最小値を使用する場合、ONTAPはこのワークロードを制限することがあり、その結果レイテンシが高くなります。

これらの水平線は、マウスオーバー時の遅延中心内訳には表示されません。これらは参照閾値として機能するものであり、レイテンシの原因となるものではありません。

I/Oタイプ別のレイテンシの内訳

「View」ドロップダウンから「Breakdown by delay center」を選択した後、「Latency Analysis」セクションのI/Oタイプの内訳を使用してください。このグラフは、I/O操作の方向に基づいて、総レイテンシを3つのカテゴリに分類します。これらの指標を使用して、パフォーマンスの問題が読み取り、書き込み、またはメタデータ操作に影響しているかどうかを判断します。

レイテンシータイプ	説明	値上昇の一般的な原因
読み取りレイテンシ	クライアントからのボリューム読み取りリクエストが完了するまでの平均時間。リクエストを受信してからデータが返されるまでの時間を示します。読み取りリクエストは、ネットワーク プロトコル層からデータ処理スタックを経由して、データが存在するアグリゲートまで、完全なI/Oパスを通過する必要があります。	集約またはディスク競合、キャッシュミスによる物理ディスクへの読み取りの増加、FabricPool 経由でクラウド容量層から取得されたコールドデータ、データがリクエストを処理するノードとは異なるノードに存在する場合のクロスノード読み取り。
書き込みレイテンシ	ボリュームに対するクライアント書き込みリクエストを承認するまでの平均時間。ONTAPは、書き込みがNVRAM書き込みログにコミットされると、書き込みを承認します。データは後でアグリゲートにフラッシュされます。	NICの飽和状態、またはクライアントとストレージ ノード間の往復遅延が大きい場合；同期SnapMirrorが書き込みを確認応答する前に、デスティネーション クラスタからの受領確認を待機している場合；書き込み負荷が高い場合のNVRAMへの圧力；書き込みI/Oパスで実行されるインライン重複排除、圧縮、またはコンパクションによるCPUオーバーヘッド。

レイテンシータイプ	説明	値上昇の一般的な原因
その他の遅延	ボリューム上での読み取り・書き込み以外の操作（ファイルオープン、属性検索、ディレクトリ走査、ファイル作成、ロックなど）の完了にかかる平均時間。読み取りおよび書き込みのレイテンシが正常に見えても、その他のレイテンシが増加すると、アプリケーションの応答性に影響を与える可能性があります。	メタデータ処理と競合するインライン効率化操作によるCPU負荷。大量のファイル作成、削除、またはディレクトリスキャンを生成するワークロードによる高いネームスペースアクティビティ。合計IOPSを制限するQoSスロットリングにより、メタデータ操作に使用できるIOPSが少なくなる。多数のボリュームが同時にアクティブになっている場合のボリュームアクティベーションのオーバーヘッド。

スループットコンポーネント

「表示」ドロップダウンから「内訳（RWO）」を選択した後、*スループット分析*セクションのスループットコンポーネントを使用してください。このアナライザーは、IOPSとMB/sの両方を同時に表示します。

コンポーネント	説明	レンダリング結果
Read IOPS	1秒あたりの読み取り操作数。	IOPSチャート上の積み重ね領域。
Write IOPS	1秒あたりの書き込み操作数。	IOPSチャート上の積み重ね領域。
IOPS：その他	メタデータおよびその他の非データ操作（1秒あたり）	IOPSチャート上の積み重ね領域。
読み取りMB/s	読み取りスループット（メガバイト/秒）	MB/sグラフの積み上げ面。
書き込み MB/s	書き込みスループット（メガバイト/秒）。	MB/sグラフの積み上げ面。
クラウド スループット	ボリュームとクラウド容量層間のスループット（メガバイト/秒）。このメトリックは、FabricPool を通じてクラウドに容量をティアリングするワークロードに対してのみ表示されます。	MB/sグラフの積み上げ面。

読み取り、書き込み、その他のコンポーネントを合計したものが、総IOPS値またはMB/s値となります。グラフにカーソルを合わせると、各コンポーネントの値、合計に対する割合、およびカテゴリ別の平均I/Oサイズ（MB/s ÷ IOPS）が表示されます。

リソース利用率指標

リソース利用状況の指標を確認するには、*リソース利用状況*セクションを使用してください。アナライザーは、ボリュームにサービスを提供する各リソースを独立した行として表示します。リソースは重複して使用できません。

ノードメトリクス

指標	説明
ノード利用率	ノードの複合利用率。各ノードにカーソルを合わせると、CPU使用率、ネットワーク使用率、および利用可能な余裕容量が表示されます。
CPU利用率	ノードのCPU使用率。ホバーツールチップにこの値が表示されます。

指標	説明
ネットワーク利用率	ノードネットワーク容量のうち、使用されている割合。ホバーツールチップにこの値が表示されます。
ヘッドルーム	追加のワークロードに使用可能な残りのノード容量。ホバーツールチップにこの値が表示されます。

集計指標

指標	説明
アグリゲートの利用率	アグリゲートのディスク使用率（%）。カーソルを合わせると、ディスク使用率、アグリゲート上のボリューム数、および利用可能な空き容量が表示されます。
ディスクがビジー状態です	アグリゲートのディスクがI/Oをアクティブに処理している時間の割合。ホバーツールチップにこの値が表示されます。
ボリュームカウント	現在、アグリゲート上でホストされているボリュームの数。ホバーツールチップにこの値が表示されます。
ヘッドルーム	追加のワークロードに使用可能な残りのアグリゲート容量。ホバーツールチップにこの値が表示されます。

ノードまたはアグリゲートの使用率ラインが、グラフ上で破線の参照線で示されている高使用率警告しきい値を超えると、そのリソース上の他のワークロードが、選択されたボリュームとI/O容量を競合している可能性があります。

容量指標

容量ビュー

「表示」ドロップダウンから「容量ビュー」を選択した後、*容量分析*セクションを使用して容量ビューのメトリックを確認してください。

指標	説明
物理容量	ストレージ効率化処理後のディスク使用量。これは、グラフの一番下の積み重ねられた領域です。物理容量＋利用可能容量は常に総容量と等しくなります。
使用可能容量	ボリューム内の残り空き容量。これは、グラフの最上部に積み重ねられた領域です。物理容量が増加するにつれて、その値は減少します。
ストレージ効率比	総合効率比（論理データ÷物理データ）。ホバーツールチップにこの値が表示されます。これは、重複排除、圧縮、およびコンパクションによる総合的な節約効果を反映したものです。
重複排除による節約効果	重複するデータブロックを削除することで節約された容量。ホバーツールチップにこの値が表示されます。
圧縮による節約効果	データをインラインで圧縮することで節約された容量。ホバーツールチップにこの値が表示されます。
圧縮による節約効果	複数の小さなブロックを1つの物理ブロックにパックすることで節約されたスペース。ホバーツールチップにこの値が表示されます。

Snapshot ビュー

スナップショット固有の指標を確認したい場合は、スナップショットビューを使用してください。

指標	説明	レンダリング結果
利用可能なスナップショット	スナップショット用に事前に割り当てられた領域。ボリュームサイズの割合として設定されます。	水平基準線。
使用済みスナップショット	スナップショットのコピーによって実際に消費される容量。	予備線下のエリアチャート。

グラフにカーソルを合わせると、スナップショットのリザーブサイズ、使用されているスナップショット領域とそのリザーブ全体に対する割合、スナップショットの総数、および最も古いスナップショットの経過時間が表示されます。スナップショットの使用量が予約容量を超えると、スナップショットはボリュームのデータ領域から容量を消費し始めます。

予測の動作

観測された傾向に基づいて現在時刻以降の将来の値を予測したい場合は、分析セクションの **Show Forecast** トグルを使用してください。以下の動作は、すべてのセクションに適用されます。

側面	動作
投影窓	選択した時間範囲に基づいて予測します。2時間ビューの場合、予測ウィンドウは約1時間です。7日間ビューの場合、予測ウィンドウは数日間にわたります。
ビジュアルスタイル	アナライザーは予測値を破線で表示します。垂直の区切り線は、実際のデータと予測値の境界を示します。
しきい値アラート	分析ツールは、予測結果からボリュームが警告または重大なしきい値を超えることが示された場合、そのしきい値を超えるまでの推定時間とともに、インサイトメッセージを表示します。
トレンドベース	この予測では、選択した期間のうち直近の部分における変化率を使用します。最近のデータの変動性が高い場合、予測の信頼性が低下します。
必要最低限のデータ	容量予測には少なくとも10日間の履歴データが必要です。容量が満杯になるまでの残り日数が30日未満になると、アナライザーはストレージがほぼ満杯であると認識します。

関連情報

- "NetApp Console ローカル展開ワークロードアナライザーについて"
- "ボリュームの高遅延を調査する"
- "ボリュームの高スループット要求を調査する"
- "ボリュームの容量増加を調査する"

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。

参照先

NetApp Console ローカルデプロイメント API

NetApp Console のローカル展開組織とフリート ID を管理する

NetApp Console のローカル展開では、NetApp Console の組織には名前と ID があります。組織を識別するために、組織名を決めることができます。特定の連携においては、組織 ID を取得する必要がある場合もあります。

必要なアクセスロール

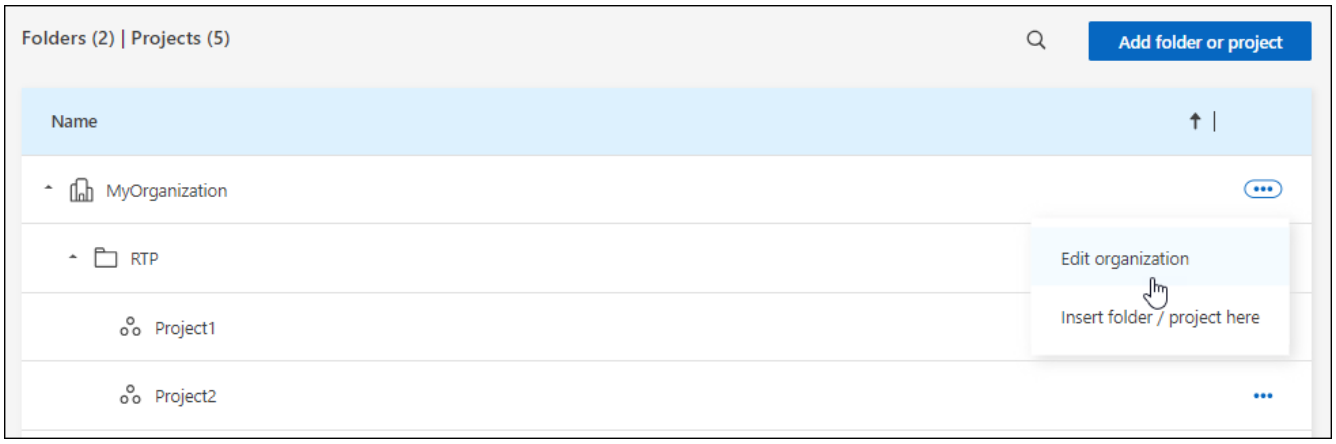
スーパー管理者または組織管理者。"アクセスロールについて"。

組織名を変更する

組織名を変更できます。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. **Organization** を選択します。
3. 「組織」ページから、テーブルの最初の行に移動し、•••を選択して、「組織の編集」を選択します。



4. 新しい組織名を入力し、**Apply** を選択してください。

組織IDを取得する

組織IDは、コンソールとの特定の連携に使用されます。

組織IDは「組織」ページから確認でき、必要に応じてクリップボードにコピーできます。

手順

1. **Administration**（管理） ＞ **Identity and access**（IDとアクセス） ＞ **Organization**（組織） を選択します。
2. 「組織」ページで、概要バーにある組織IDを探し、クリップボードにコピーしてください。後で使用するために保存することも、必要な場所に直接コピーすることもできます。

フリートのIDを取得する

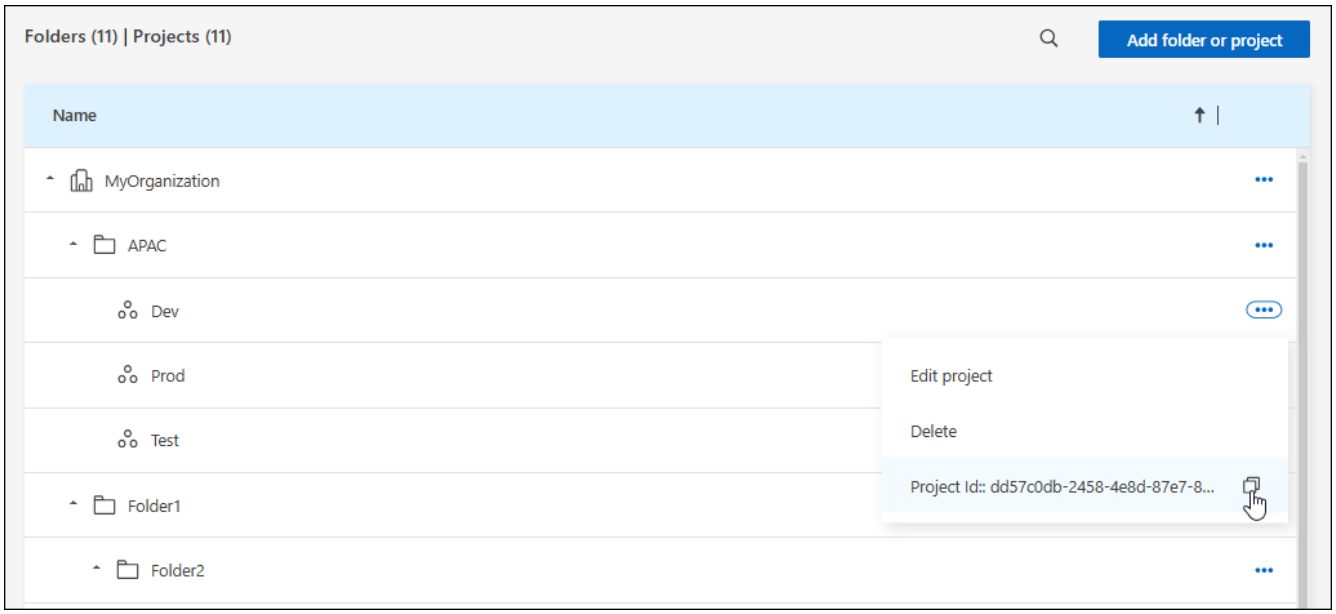
APIを使用する場合は、フリートのIDを取得する必要があります。

手順

1. 「組織」ページから、表内のフリートに移動して ••• を選択します。

   フリート ID が表示されます。

2. IDをコピーするには、コピーボタンを選択してください。



関連情報

- "アイデンティティとアクセス管理について"
- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "IDとアクセス管理のAPIについて"

サポートされているLLMプロバイダーとモデル（NetApp Console ローカル展開）

NetApp Console のローカル展開では、OpenAI、OpenAI 互換、および Anthropic LLM プ

ロバイダータイプがサポートされています。選択できるモデルは、設定するプロバイダータイプとエンドポイントによって異なります。

> LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

パフォーマンス、コスト、ガバナンスに関する要件に合ったモデルを選択してください。

プロバイダーの種類がモデルの可用性にどのように影響するかを確認してください

選択したプロバイダーの種類によって、Console のローカルデプロイメントモデルリストに表示されるモデルが決まります。

- **OpenAI** — OpenAIと直接統合するためのモデルを提供します。
- **OpenAI**互換 — 組織の互換エンドポイントが公開するモデルを提供します。
- **Anthropic** — 直接的な Anthropic 統合のためのモデルを提供します。

表示されるモデルは、エンドポイントの設定、プロキシまたはゲートウェイの動作、および組織のポリシーによって異なる場合があります。プロバイダーの種類は、接続先のエンドポイントと、そのエンドポイントが公開するモデルによって異なり、トランスポートプロトコルによって異なるわけではありません。

サポートされている**OpenAI**モデル

- GPT-5.4
- GPT-5.5

サポートされている **Anthropic** モデル

- Claude Sonnet 4.6
- Claude Opus 4.6、4.7 & 4.8

関連情報

- "LLMを接続してNetApp Consoleアシスタントを有効にする".
- "NetApp Console ローカル展開における LLM 統合について".

ONTAP アラートリファレンス（NetApp Console ローカル展開）

このリファレンスでは、NetApp Console のローカル展開が監視できる ONTAP アラートを、影響度カテゴリ別に整理して一覧表示しています。

重大度マッピング

同じ EMS アラートでも、それを引き起こした ONTAP イベントに応じて、重大、警告、または情報として表示される場合があります：

- **Critical**: ONTAPの重大度からマッピング `alert`、 `emergency`

- 警告：ONTAPの重大度からのマップ `error`
- 情報: ONTAPの重大度からマッピング `notice`、 `informational`
- その他：そのまま通過

動的マッピングにより、単一のアラートルールが、EMSイベントの実行時コンテキストに応じて異なる重大度を出力できるようになります。

以下のセクションでは、アラートを影響度カテゴリ別に分類し、各表をアラート名のアルファベット順に並べ替えています。

可用性アラート

これらのアラートは、システム、サービス、またはデータの可用性に影響を与える可能性があります。

アラート名	重大度	**Type**	説明
Active Directoryサーバーへの接続が切断されました	重大	EMS	このSVM用に設定されているすべてのAD/LDAPサーバーにアクセスできません。
アグリゲートはオンラインではありません	重大	指標	一部のアグリゲートがオフラインです。ボリュームを作成すると、FSIDが重複する可能性があります。
ウイルス対策サーバーがビジー状態です	重大、警告、情報	EMS	ウイルス対策サーバーが過負荷状態のため、追加のスキャン要求を受け付けることができません。
AWS認証情報が初期化されていません	重大、警告、情報	EMS	モジュールが、初期化前にAWS IAMのロールベースの認証情報へのアクセスを試みました。
クラウド層にアクセスできません	重大、警告、情報	EMS	ストレージ ノードがCloud Tierオブジェクトストアに接続できません。一部のデータにはアクセスできません。
ディスク障害	重大	指標	ディスクに障害が発生したか、ディスク消去処理中であるか、またはメンテナンスモードになっています。
ディスクが使用不能です	重大、警告、情報	EMS	ディスクは、故障、データ消去、またはメンテナンスのため、使用停止となりました。
ディスク シェルフの電源ユニットが取り外されました	重大、警告、情報	EMS	電源ユニットがディスク シェルフから取り外されました。
FCターゲットポートコマンドが超過しました	重大、警告、情報	EMS	物理FCターゲットポート上の未処理コマンド数が、サポートされている制限を超えています。
ストレージプールの返却に失敗しました	重大、警告、情報	EMS	このイベントは、ストレージフェイルオーバー（SFO）のギブバックの一環としてストレージプール（アグリゲート）を再配置する際に、宛先ノードがオブジェクトストアにアクセスできない場合に発生します。

アラート名	重大度	**Type**	説明
HAインターコネクトがダウン	重大、警告、情報	EMS	HAインターコネクトがダウンしています。フェイルオーバーが利用できない場合、サービス停止のリスクがあります。
InstanceDown	重大	指標	監視対象のインスタンスにアクセスできません。ダウンしているか、ネットワークの問題が発生している可能性があります。
LUNが削除されました	重大、警告、情報	EMS	LUNが破壊され、アクセスできなくなりました。
LUNオフライン	重大、警告、情報	EMS	LUNが手動でオフラインにされました。
本体ファンが故障しました	重大、警告、情報	EMS	メインユニットのファンが1つ以上故障しました。システムは引き続き稼働しています。
本体ファンが警告状態です	重大、警告、情報	EMS	本体冷却ファンのうち1つ以上が警告状態です。
ユーザーあたりの最大セッション数を超えました	重大、警告、情報	EMS	TCP接続におけるユーザーあたりの最大セッション数を超えました。
ファイルごとの最大オープン回数を超えました	重大、警告、情報	EMS	TCP接続を介してファイルを開くことができる最大回数を超えました。
MetroCluster 自動計画外スイッチオーバーが無効になっています	重大、警告、情報	EMS	このクラスターでは、自動計画外スイッチオーバー機能が無効になっています。
MetroClusterの監視	重大、警告、情報	EMS	システムヘルスモニターのアラートが検出されました。
NFSv4ストアプールが枯渇しました	重大、警告、情報	EMS	NFSv4ストアプールが枯渇しました。
NetBIOS名の競合	重大、警告、情報	EMS	NetBIOS ネームサービスは、リモートマシンからの名前登録要求に対して否定応答を受信しました。
登録されたスキャンエンジンがありません	重大、警告、情報	EMS	アンチウイルスコネクタは、登録済みのスキャンエンジンがないことを ONTAP に通知しました。
Vscan接続なし	重大、警告、情報	EMS	ONTAPには、ウイルス スキャン要求に対応するためのVscan接続がありません。スキャン必須オプションが有効になっている場合、データが利用できなくなる可能性があります。
応答しないウイルス対策サーバー	重大、警告、情報	EMS	ONTAPは応答しないウイルス対策サーバーを検出し、Vscan接続を強制的に切断しました。
存在しない管理者共有	重大、警告、情報	EMS	Vscanの問題：クライアントが、存在しないONTAP_ADMIN$共有に接続しようとしました。

アラート名	重大度	Type	説明
NVRAMバッテリー残量低下	重大、警告、情報	EMS	NVRAM バッテリー容量が極めて低下しています。バッテリーが切れた場合、データが失われる可能性があります。
NVMe名前空間が破棄されました	重大、警告、情報	EMS	NVMeネームスペースが破壊され、アクセスできなくなりました。
NVMe名前空間がオフライン	重大、警告、情報	EMS	NVMeネームスペースが手動でオフラインにされました。
NVMeネームスペースオンライン	重大、警告、情報	EMS	NVMeネームスペースがオンラインに復旧しました。
NVMe-oFライセンスの猶予期間が有効です	重大、警告、情報	EMS	このイベントは、NVMe over Fabrics（NVMe-oF）プロトコルが使用されており、かつライセンスの猶予期間が有効な場合に毎日発生します。
NVMe-oFライセンスの猶予期間が終了しました	重大、警告、情報	EMS	NVMe over Fabrics（NVMe-oF）のライセンス猶予期間が終了し、NVMe-oF機能は無効になりました。
NVMe-oFライセンスの猶予期間開始	重大、警告、情報	EMS	NVMe over Fabrics （NVMe-oF）構成は、ONTAP 9.5ソフトウェアへのアップグレード中に検出されました。
オブジェクトストアホストを解決できません	重大、警告、情報	EMS	オブジェクトストアサーバーのホスト名をIPアドレスに解決できません。
オブジェクトストアのクラスタ間LIFがダウン	重大、警告、情報	EMS	オブジェクトストアクライアントは、オブジェクトストアサーバーと通信するための動作可能なLIFを見つけることができません。
オブジェクトストアの署名が一致しません	重大、警告、情報	EMS	オブジェクトストアサーバーに送信されたリクエスト署名が、クライアントによって計算された署名と一致しません。
ポート ステータス - 停止	重大	EMS	このイーサネットポートはダウンしています。そのリンクのトラフィックに影響が出る可能性があります。
READDIRタイムアウト	重大、警告、情報	EMS	READDIRファイル操作の実行時間が、WAFLで許可されているタイムアウトを超えました。
ストレージプールの再配置に失敗しました	重大、警告、情報	EMS	このイベントは、ストレージプール（アグリゲート）の再配置中に、宛先ノードがオブジェクトストアにアクセスできない場合に発生します。
SAN アクティブ / アクティブ状態が変わりました	重大、警告、情報	EMS	SANのパス構成はもはや対称ではありません。
サービスプロセッサのハートビートが欠落しました	重大、警告、情報	EMS	ONTAP は、Service Processor （SP）から予期されるハートビート信号を受信していません。

アラート名	重大度	Type	説明
Service Processor のハートビートが停止しました	重大、警告、情報	EMS	ONTAPはService Processor（SP）からハートビートを受信しなくなりました。
サービスプロセッサが構成されていません	重大、警告、情報	EMS	このイベントは毎週発生し、Service Processor（SP）を設定するよう通知します。
サービスプロセッサがオフラインです	重大、警告、情報	EMS	サービスプロセッサ（SP）はオフラインです。
FC ターゲット アダプタの SFP が低電力を受信しています	重大、警告、情報	EMS	このアラートは、小型フォームファクタのプラグイン式トランシーバ（FCターゲットのSFP）が受信する電力（RX）が、定義されたしきい値を下回った場合に発生します。
FCターゲット アダプタのSFPが低電力で送信中	重大、警告、情報	EMS	このアラートは、小型フォームファクタのプラグイン式トランシーバ（FCターゲットではSFP）が送信する電力（TX）が、定義されたしきい値を下回った場合に発生します。
シャドウコピーに失敗しました	重大、警告、情報	EMS	Microsoft Serverのバックアップおよび復元サービスであるボリューム シャドウ コピー サービス（VSS）の操作が失敗しました。
シェルフファンに障害が発生しました	重大、警告、情報	EMS	シェルフの該当する冷却ファンまたはファンモジュールに障害が発生しました。
SnapMirror のラグタイムが長い	重大	指標	SnapMirror関係の更新が予定スケジュールより1時間以上遅れています。
ストレージ フェイルオーバー インターコネクトの 1 つ以上のリンクが停止	警告	EMS	1つ以上のHAインターコネクトのパートナーノードへのリンクがダウンしています。フェイルオーバーの冗長性が低下しています。
ストレージスイッチの電源が故障しました	重大、警告、情報	EMS	クラススイッチの電源装置が不足しています。冗長性が低下しています。
ストレージVMの停止に成功しました	重大、警告、情報	EMS	ストレージVMは正常に停止しました。
SVM構成レプリケーションライセンスが無効です	警告	EMS	SVM-DR構成レプリケーションライセンスが欠落しているか、期限切れであるか、または適用されていません
本体ファンの故障により、システムは動作できません。	重大、警告、情報	EMS	本体ファンが1つ以上故障し、システムの動作に支障が出ています。これはデータ損失につながる可能性があります。
CIFS認証が多すぎます	重大、警告、情報	EMS	多数の認証ネゴシエーションが同時に発生しました。このクライアントからの未完了の新規セッションリクエストが256件あります。
ディスクが割り当てられていない	重大、警告、情報	EMS	システムに未割り当てのディスクがあり、容量が無駄になっています。
ボリュームの状態がオフラインです	情報	指標	当該ボリュームはオフラインになりました。

アラート名	重大度	Type	説明
ボリュームは制限状態	重大、警告、情報	EMS	このイベントは、フレキシブル ボリュームが制限付きに設定されたことを示します。
ウイルスが検出されました	重大、警告、情報	EMS	Vscanサーバーが、ファイルがウイルスに感染している可能性があると報告しました。

容量のアラート

これらのアラートは、ストレージの使用状況または容量不足を示しています。

アラート名	重大度	Type	説明
FabricPoolミラーレプリケーションの再同期が完了しました	重大、警告、情報	EMS	FabricPoolのミラー再同期処理が、プライマリオブジェクトストアからミラーオブジェクトストアへ正常に完了しました。
FabricPool スペース使用制限にほぼ達しました	重大、警告、情報	EMS	クラスター全体の、容量ライセンスプロバイダーのオブジェクトストアの FabricPool 合計スペース使用量がライセンスの上限にほぼ達しました。
FabricPoolスペース使用制限に達しました	重大、警告、情報	EMS	クラスター全体のFabricPoolにおける、容量ライセンスプロバイダーのオブジェクトストアの合計スペース使用量がライセンスの上限に達しました。
ノードルートボリュームの空き容量が少ない	重大、警告、情報	EMS	システムは、ルートボリュームの空き容量が危険なほど不足していることを検出しました。
QoSモニターのメモリが最大容量に達しました	重大、警告、情報	EMS	QoSサブシステムの動的メモリが、現在のプラットフォームハードウェアの限界に達しました。
ボリュームの自動サイズ変更が成功しました	重大、警告、情報	EMS	ボリュームの自動拡張が有効になっているため、ボリュームのサイズが自動的に変更されました。
ボリュームがいっぱいです	重大	指標	容量は90%以上埋まっています。書き込みエラーを防ぐため、空き容量を確保するか、容量を追加してください。

設定アラート

これらのアラートは、設定変更または在庫更新を示しています。

アラート名	重大度	Type	説明
ディスク シェルフの電源が検出されました	重大、警告、情報	EMS	電源ユニットがディスク シェルフに追加されました。
ボリュームが作成されました	情報	指標	ボリュームが作成されました。
ボリュームが削除されました	警告	指標	ボリュームが削除されました。

アラート名	重大度	Type	説明
ボリュームが変更されました	情報	指標	ボリュームが変更されました。
WAFL 整合性チェックの期限超過	警告	EMS	このアグリゲートに対する WAFL 整合性チェックが、1時間あたりの制限を超えました。

パフォーマンスアラート

これらのアラートは、レイテンシまたはノードのパフォーマンスの問題を示しています。

アラート名	重大度	Type	説明
ノードNFSのレイテンシが高い	重大	指標	このノードにおけるNFS操作で、高いレイテンシ（5000マイクロ秒以上）が発生しています。
ノードのパニック	重大、警告、情報	EMS	ノードがパニック状態になり、再起動されました。

保護アラート

これらのアラートは、レプリケーション、フェイルオーバー、またはリカバリに影響します。

アラート名	重大度	Type	説明
ファンアウトSnapMirror関係の共通スナップショットが削除されました	重大、警告、情報	EMS	古いSnapshotコピーは、SnapMirror Synchronous の再同期または更新操作の一部として削除されます。
ONTAP Mediator が追加されました	重大、警告、情報	EMS	ONTAP メディエーターがこのクラスターに正常に追加されました。
ONTAPメディエーターCA証明書の有効期限が切れました	重大、警告、情報	EMS	ONTAP メディエーター認証局（CA）の証明書の有効期限が切れています。
ONTAP Mediator CA証明書の有効期限が近づいています	重大、警告、情報	EMS	ONTAP Mediator認証局（CA）の証明書は、今後30日以内に有効期限が切れます。
ONTAP Mediator クライアント証明書の有効期限が切れました	重大、警告、情報	EMS	ONTAP Mediator クライアント証明書の有効期限が切れています。
ONTAP Mediator クライアント証明書の有効期限が近づいています	重大、警告、情報	EMS	ONTAP Mediator クライアント証明書は、今後30日以内に有効期限が切れます。
ONTAP Mediatorにアクセスできません	重大、警告、情報	EMS	ONTAP Mediator にアクセスできません。これは、Mediator が別の用途に変更されたか、Mediator パッケージがインストールされなくなったためです。
ONTAP Mediator が削除されました	重大、警告、情報	EMS	ONTAP メディエーターはこのクラスターから正常に削除されました。

アラート名	重大度	Type	説明
ONTAP Mediator に到達できません	重大、警告、情報	EMS	ONTAP メディエーターに到達できません。つまり、接続が復旧するまで SnapMirror フェイルオーバーは実行できません。
ONTAPメディエーターサーバー証明書の有効期限が切れました	重大、警告、情報	EMS	ONTAP Mediatorサーバー証明書の有効期限が切れました。
ONTAP Mediator サーバー証明書の有効期限が近づいています	重大、警告、情報	EMS	ONTAP Mediatorサーバー証明書は、今後30日以内に有効期限が切れます。
SnapMirror アクティブ同期の関係が同期していません	重大、警告、情報	EMS	SnapMirror同期関係が同期中から非同期に移行しました。データ保護に影響があります。
SnapMirror アクティブ同期の自動計画外フェイルオーバーが完了しました	重大、警告、情報	EMS	SnapMirror Business Continuity （SMBC） の自動計画外フェイルオーバー操作が完了しました。
SnapMirror アクティブ同期の自動計画外フェイルオーバーが失敗しました	重大、警告、情報	EMS	SnapMirror Business Continuity （SMBC） の自動計画外フェイルオーバー操作が失敗しました。
SnapMirror アクティブ同期の計画フェイルオーバーが完了しました	重大、警告、情報	EMS	SnapMirror Business Continuity （SMBC） の計画フェイルオーバー操作が完了しました。
SnapMirror アクティブ同期の計画的フェイルオーバーが失敗しました	重大、警告、情報	EMS	SnapMirror Business Continuity （SMBC） の計画的フェイルオーバー操作が失敗しました。
SnapMirror関係の共通スナップショットが失敗しました	重大、警告、情報	EMS	共通スナップショットコピーの作成に失敗しました。
SnapMirror関係の初期化に失敗しました	重大、警告、情報	EMS	SnapMirror の初期化コマンドが失敗し、これ以上の再試行は行われません。
SnapMirror 関係が同期していない	重大、警告、情報	EMS	SnapMirror同期関係が同期中から非同期に移行しました。データ保護に影響があります。
SnapMirror 関係の再同期の試行が失敗しました	重大、警告、情報	EMS	ソースボリュームと宛先ボリューム間の SnapMirror 同期試行が失敗しました。
SnapMirrorリレーションシップのスナップショットは複製されません	重大、警告、情報	EMS	SnapMirror Synchronous 関係のSnapshotコピーが正常にレプリケートされませんでした。

セキュリティ警告

これらの警告は、脅威または不正アクセスを示しています。

アラート名	重大度	Type	説明
ランサムウェアの活動が検出されました	重大、警告、情報	EMS	検出されたランサムウェアからデータを保護するため、元のデータを復元するために使用できるSnapshotコピーが作成されました。
ストレージVMのランサムウェア対策監視	重大、警告、情報	EMS	ストレージVMのランサムウェア対策状態が変更されました。
管理者共有への不正アクセス	重大、警告、情報	EMS	クライアントが特権共有であるONTAP_ADMIN$に接続しようとしましたが、ログインしているユーザーはこのSVM上のアクティブなVscanスキャナプールに含まれていません。
ボリュームのランサムウェア対策監視	重大、警告、情報	EMS	ボリュームのランサムウェア対策状態が変更されました。

NetApp Console ローカル展開におけるクラスターセキュリティコンプライアンスカテゴリ

このリファレンスを使用して、NetApp Console のローカル展開に表示されるクラスタセキュリティコンプライアンスカテゴリを確認してください。推奨値や各カテゴリが全体的なコンプライアンス状況に影響を与えるかどうかについても説明します。

これらのカテゴリーは、ONTAPセキュリティ態勢チェックに基づいています。

カテゴリ	このカテゴリがチェックする内容	推奨値	全体的なコンプライアンスに影響を与える
グローバル FIPS	FIPS 140-2モードが有効になっているかどうか。有効にすると、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが許可されます。	有効	はい
Telnet	Telnetアクセスが有効になっているかどうか。SSHは、推奨される安全なリモートアクセス方法です。	Disabled	はい
安全でないSSH設定	SSHが安全でない暗号（例えば、 `cbc`で始まる暗号）で構成されているかどうか。	×	はい
ログイン バナー	システムアクセスにログインバナーが設定されているかどうか。	有効	はい
クラスタ ピアリング	ピアリングされたクラスター間の通信が暗号化されているかどうか。暗号化は、送信元クラスターと送信先クラスターの両方で有効にする必要があります。	暗号化	はい
ネットワーク タイム プロトコル	クラスター用に1つ以上のNTPサーバーが構成されているかどうか。NetAppでは、耐障害性を確保するため、少なくとも3つのNTPサーバーを推奨します。	設定	はい
OCSP	SSL/TLS証明書の検証において、オンライン証明書ステータスプロトコル（OCSP）の検証が有効になっているかどうか。	有効	×

カテゴリ	このカテゴリがチェックする内容	推奨値	全体的なコンプライアンスに影響を与える
リモート監査ログ	ログ転送（syslog）が暗号化されているかどうか。	暗号化	はい
AutoSupport HTTPSトランスポート	HTTPSがAutoSupportメッセージのデフォルトのトランスポートプロトコルとして使用されるかどうか。	有効	はい
デフォルトの管理者ユーザー	組み込みのデフォルト管理者アカウントが無効になっているかどうか。	Disabled	はい
SAMLユーザ	SAMLがシングル サインオンおよびMFA対応認証用に構成されているかどうか。	×	×
Active Directoryユーザー	クラスターアクセス用にActive Directory認証が構成されているかどうか。	×	×
LDAPユーザ	クラスタアクセス用にLDAP認証が設定されているかどうか。	×	×
証明書ユーザー	証明書ベースのユーザーがクラスタログイン用に構成されているかどうか。	×	×
ローカル ユーザ	ローカルユーザーがクラスタログイン用に設定されているかどうか。	×	×
リモートシェル	RSHが有効になっているかどうか。安全なリモートアクセスにはSSHが推奨されます。	Disabled	はい
MD5が使用されています	ONTAP ユーザーアカウントが、SHA-512 などのより強力なハッシュではなく、依然として MD5 ハッシュを使用しているかどうか。	×	はい
証明書発行者タイプ	クラスターで使用される証明書発行者タイプ。	CA署名	×

ストレージ**VM**セキュリティコンプライアンスカテゴリ（**NetApp Console** ローカル展開）

このリファレンスを使用して、NetApp Console のローカル展開に表示されるストレージ VM （SVM） のセキュリティコンプライアンスカテゴリを確認してください。推奨値や各カテゴリが全体的なコンプライアンス状況に影響を与えるかどうかについても説明します。

これらのカテゴリーは、ONTAPセキュリティ態勢チェックに基づいています。

カテゴリ	このカテゴリがチェックする内容	推奨値	全体的なコンプライアンスに影響を与える
監査ログ	SVM監査ログが有効になっているかどうか。	有効	はい
安全でないSSH設定	SSHが安全でない暗号（例えば、 `cbc`で始まる暗号）で構成されているかどうか。	×	はい

カテゴリ	このカテゴリがチェックする内容	推奨値	全体的なコンプライアンスに影響を与える
ログイン バナー	SVMにアクセスするユーザーに対してログインバナーが設定されているかどうか。	有効	はい
LDAP暗号化	LDAP暗号化が有効になっているかどうか。	有効	×
NTLM認証	NTLM認証が有効になっているかどうか。	有効	×
LDAPペイロード署名	LDAPペイロード署名が有効かどうか。	有効	×
CHAP設定	CHAPが有効になっているかどうか。	有効	×
Kerberos V5	Kerberos V5認証が有効になっているかどうか。	有効	×
NIS認証	NIS認証が設定されているかどうか。	Disabled	×
FPolicy ステータス：アクティブ	FPolicyが作成され、有効になっているかどうか。	はい	×
SMB暗号化が有効になっています	SMBの署名とシーリングが有効になっているかどうか。	はい	×
SMB署名が有効になっています	SMB署名が有効になっているかどうか。	はい	×

ナレッジとサポート

NetApp Console ローカル展開でサポートに登録する

NetApp Console のこのタスクのローカル展開情報です。NetApp Console およびそのストレージソリューションとデータサービスに関する技術サポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAP システムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウド プロバイダのファイルサービスに対する NetApp のサポートは有効になりません。クラウド プロバイダのファイルサービス、そのインフラストラクチャ、またはそのサービスを使用するソリューションに関するテクニカルサポートについては、該当製品のドキュメントにある「ヘルプの入手」を参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

サポート登録の概要

サポートの利用資格を有効化するための登録方法は2種類あります。

- NetApp Console アカウントのシリアル番号（Console のサポートリソースページに記載されている 20 桁の 960xxxxxxxx シリアル番号）を登録します。

これは、コンソール内のあらゆるサービスにおける、お客様専用のサポートサブスクリプションIDとして機能します。各コンソールアカウントは登録が必要です。

- クラウド プロバイダのマーケットプレイスでサブスクリプションに関連付けられた Cloud Volumes ONTAP のシリアル番号を登録します（これらは20桁の909201xxxxxxxxシリアル番号です）。

  これらのシリアル番号は一般的に_PAYGOシリアル番号_と呼ばれ、Cloud Volumes ONTAP のデプロイ時に NetApp Console によって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットの発行や自動ケース生成などの機能が利用可能になります。登録は、以下に説明するように NetApp Support Site （NSS） アカウントをコンソールに追加することで完了します。

NetApp ConsoleをNetAppサポートに登録します

サポートに登録してサポートの利用権限を有効にするには、NetApp Console アカウントの1人のユーザーが、NetApp Support Site アカウントをコンソールのログインに関連付ける必要があります。NetApp サポートへの登録方法は、NetApp Support Site （NSS）アカウントをすでにお持ちかどうかによって異なります。

NSSアカウントをお持ちの既存顧客

NetAppのNSSアカウントをお持ちのお客様は、コンソールからサポートに登録するだけで済みます。

手順

1. **Administration** > **Credentials** を選択します。
2. 「ユーザー認証情報」を選択します。
3. 「NSS認証情報の追加」を選択し、NetApp Support Site（NSS）の認証プロンプトに従ってください。
4. 登録手続きが正常に完了したことを確認するには、ヘルプアイコンを選択し、*サポート*を選択してください。

   「リソース」ページには、Console アカウントがサポート対象として登録されていることが表示されます。

   他のコンソールユーザーが NetApp Support Site のアカウントをログインに関連付けていない場合、同じサポート登録ステータスは表示されません。ただし、これはアカウントがサポートに登録されていないことを意味するわけではありません。組織内の1人のユーザーがこれらの手順を完了していれば、アカウントは登録済みです。

既存顧客だがNSSアカウントは持っていない

既存のNetAppのお客様で、既存のライセンスとシリアル番号をお持ちであるが、NSSアカウントをお持ちでない場合は、NSSアカウントを作成し、コンソールログインに関連付ける必要があります。

手順

1. NetApp Support Site アカウントを作成するには、 "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザーレベルを選択してください。通常は **NetApp Customer/End User** です。
   b. 必ず、上記で使用したコンソールアカウントのシリアル番号（960xxxx）をコピーして、シリアル番号欄に入力してください。これにより、アカウント処理が迅速化されます。

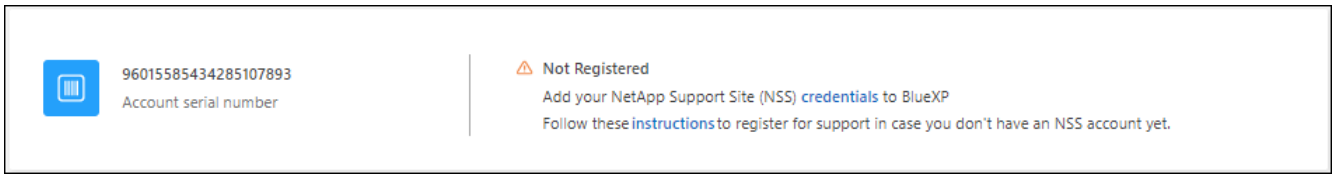
2. 以下の手順を完了して、新しいNSSアカウントをコンソールログインに関連付けてください：NSSアカウントをお持ちの既存顧客。

NetAppをご利用いただくのが初めての方へ

NetAppを初めてご利用になる方で、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. コンソールの右上にあるヘルプアイコンを選択し、*サポート*を選択します。
2. サポート登録ページからアカウントIDのシリアル番号をご確認ください。



3. "NetAppのサポート登録サイト"に移動し、*登録済みの NetApp のお客様ではありません*を選択します。
4. 必須項目（赤いアスタリスクが付いている項目）を入力してください。
5. 「Product Line」フィールドで「Cloud Manager」を選択し、該当する請求プロバイダーを選択してください。
6. 上記のステップ2のアカウントシリアル番号をコピーし、セキュリティチェックを完了してから、NetAppのグローバルデータプライバシーポリシーを読んだことを確認してください。

   この安全な取引を完了するために、ご提供いただいたメールアドレスに直ちにメールが送信されます。確認メールが数分以内に届かない場合は、迷惑メールフォルダをご確認ください。

7. メール本文から操作内容を確認してください。

   確認すると、リクエストが NetApp に送信され、NetApp Support Site アカウントを作成することをお勧めします。

8. NetApp Support Site アカウントを作成するには、 "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザーレベルを選択してください。通常は **NetApp Customer/End User** です。
   b. 必ず上記のアカウントシリアル番号（960xxxx）をコピーして、シリアル番号欄に入力してください。これにより処理速度が向上します。

終了後の操作

NetApp のサポート担当者がこのプロセス中にご連絡いたします。これは新規ユーザー向けの初回のみのオンボーディング手順です。

NetApp Support Site アカウントを取得したら、NSSアカウントをお持ちの既存顧客 の手順を完了して、アカウントをコンソールログインに関連付けてください。

Cloud Volumes ONTAP サポートのための **NSS** 資格情報の関連付け

以下の主要なワークフローを有効にするには、NetApp Support Site の認証情報をコンソール アカウントに関連付ける必要があります。Cloud Volumes ONTAP：

- 従量課金制 Cloud Volumes ONTAP システムをサポートに登録する

  システムのサポートを有効にし、NetAppテクニカルサポートリソースへのアクセスを取得するには、NSSアカウントの提供が必要です。

- 独自ライセンスを使用する場合（BYOL）の Cloud Volumes ONTAP の導入

  コンソールがライセンスキーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSSアカウントの提供が必要です。これには、契約更新時の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードする

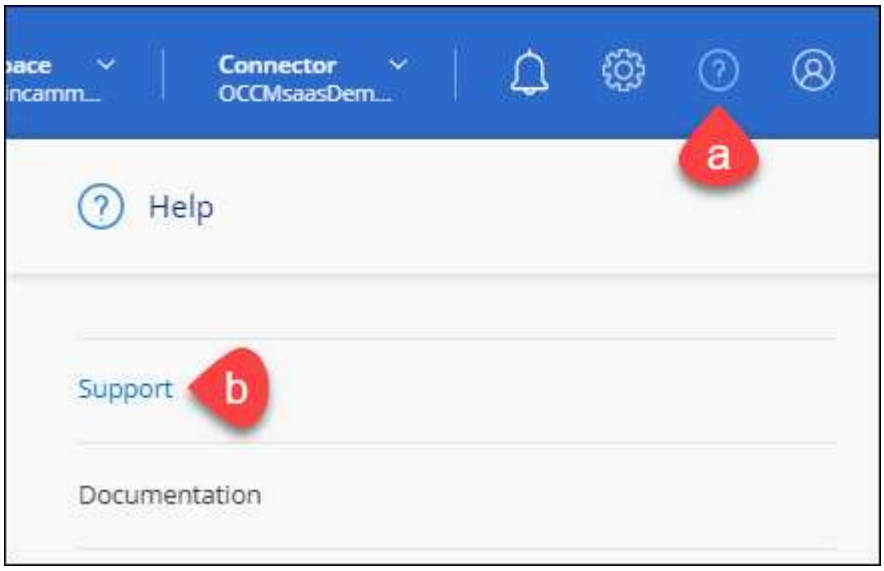
NSS 認証情報を NetApp Console アカウントに関連付けることは、Console ユーザーのログインに関連付けられている NSS アカウントとは異なります。

これらのNSS認証情報は、お客様固有のコンソールアカウントIDに関連付けられています。コンソール組織に所属するユーザーは、サポート **> NSS**管理 からこれらの認証情報にアクセスできます。

- 顧客レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加できます。
- パートナーアカウントまたは再販業者アカウントをお持ちの場合は、1つ以上のNSSアカウントを追加できますが、顧客レベルのアカウントと並行して追加することはできません。

手順

1. コンソールの右上にあるヘルプアイコンを選択し、*サポート*を選択します。



2. 「NSS Management」＞「Add NSS Account」を選択します。
3. プロンプトが表示されたら、*続行*を選択して、Microsoft のログインページにリダイレクトされます。

   NetAppは、サポートおよびライセンスに特化した認証サービスのIDプロバイダーとして、Microsoft Entra IDを使用しています。

4. ログインページで、認証プロセスを実行するために、NetApp Support Site に登録されているメールアドレスとパスワードを入力してください。

   これらの操作により、コンソールはライセンスのダウンロード、ソフトウェアのアップグレード確認、今

後のサポート登録などの目的で、お客様のNSSアカウントを使用できるようになります。

次の点に注意してください。

- NSSアカウントは、顧客レベルのアカウントである必要があります（ゲストアカウントや一時アカウントは不可）。顧客レベルのNSSアカウントは複数作成できます。
- パートナーレベルのアカウントである場合、NSSアカウントは1つしか作成できません。顧客レベルのNSSアカウントを追加しようとした際に、パートナーレベルのアカウントが既に存在する場合、次のエラーメッセージが表示されます：

  「このアカウントには既に別のタイプのNSSユーザーが登録されているため、NSS顧客タイプは許可されていません。」

既存の顧客レベルのNSSアカウントをお持ちの場合、パートナーレベルのアカウントを追加しようとする場合も同様です。

- ログインに成功すると、NetApp は NSS ユーザー名を保存します。

  これはシステムによって生成されたIDで、お客様のメールアドレスにマッピングされます。*NSS管理*ページの ••• メニューからメールアドレスを表示できます。

- ログイン資格情報トークンを更新する必要がある場合は、 ••• メニューに*資格情報の更新*オプションもあります。

  このオプションを選択すると、再度ログインを求められます。これらのアカウントのトークンは 90 日後に有効期限が切れることにご注意ください。この件については、通知が掲載されますのでご確認ください。

NetApp Consoleのローカルデプロイに関するヘルプを参照する

NetApp Console のこのタスクのローカル展開情報です。NetApp は、NetApp Console およびそのクラウドサービスをさまざまな方法でサポートしています。ナレッジベース（KB）の記事やコミュニティフォーラムなど、充実した無料のセルフサポートオプションが24時間365日利用可能です。サポート登録には、ウェブチケットによるリモート技術サポートが含まれています。

クラウド プロバイダファイルサービスのサポートを受ける

クラウド プロバイダのファイルサービス、そのインフラ、またはそのサービスを使用するソリューションに関する技術サポートについては、該当する製品のマニュアルを参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

NetAppとそのストレージソリューションおよびデータサービスに関する技術サポートを受けるには、以下に説明するサポートオプションをご利用ください。

セルフサポートオプションを利用する

これらのオプションは、24時間年中無休で無料でご利用いただけます。

- ドキュメント

  現在ご覧になっているNetApp Consoleのドキュメント。

- "ナレッジベース"

  NetApp ナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  NetApp Console コミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

NetApp サポートでケースを作成する

上記のセルフサポートオプションに加えて、サポートを有効化した後は、NetApp サポートスペシャリストと連携してあらゆる問題を解決することができます。

始める前に

- *ケースの作成*機能を使用するには、まずNetApp Support Siteの認証情報をConsoleログインに関連付ける必要があります "Console ログインに関連付けられたクレデンシャルを管理する方法について説明します。"。
- シリアル番号を持つ ONTAP システムのケースを開く場合、NSS アカウントはそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. NetApp Consoleで、*Help > Support*を選択します。
2. 「リソース」ページで、「テクニカルサポート」の下にある利用可能なオプションからいずれかを選択してください。

   a. 電話で担当者とお話しになりたい場合は、*お問い合わせください*を選択してください。netapp.com のページに移動し、お電話いただける電話番号が記載されています。

   b. 「ケースを作成」を選択して、NetApp サポートスペシャリストとのチケットを開きます：

      - サービス：問題が関連しているサービスを選択してください。たとえば、コンソール内のワークフローまたは機能に関する技術サポートの問題に特化している場合は、**NetApp Console** を選択します。
      - システム：ストレージに該当する場合は、*Cloud Volumes ONTAP*または*オンプレミス*を選択し、関連する作業環境を選択します。

        表示されているシステムは、NetApp Console組織および上部バナーで選択したNetApp Consoleエージェントの範囲内にあるシステムです。

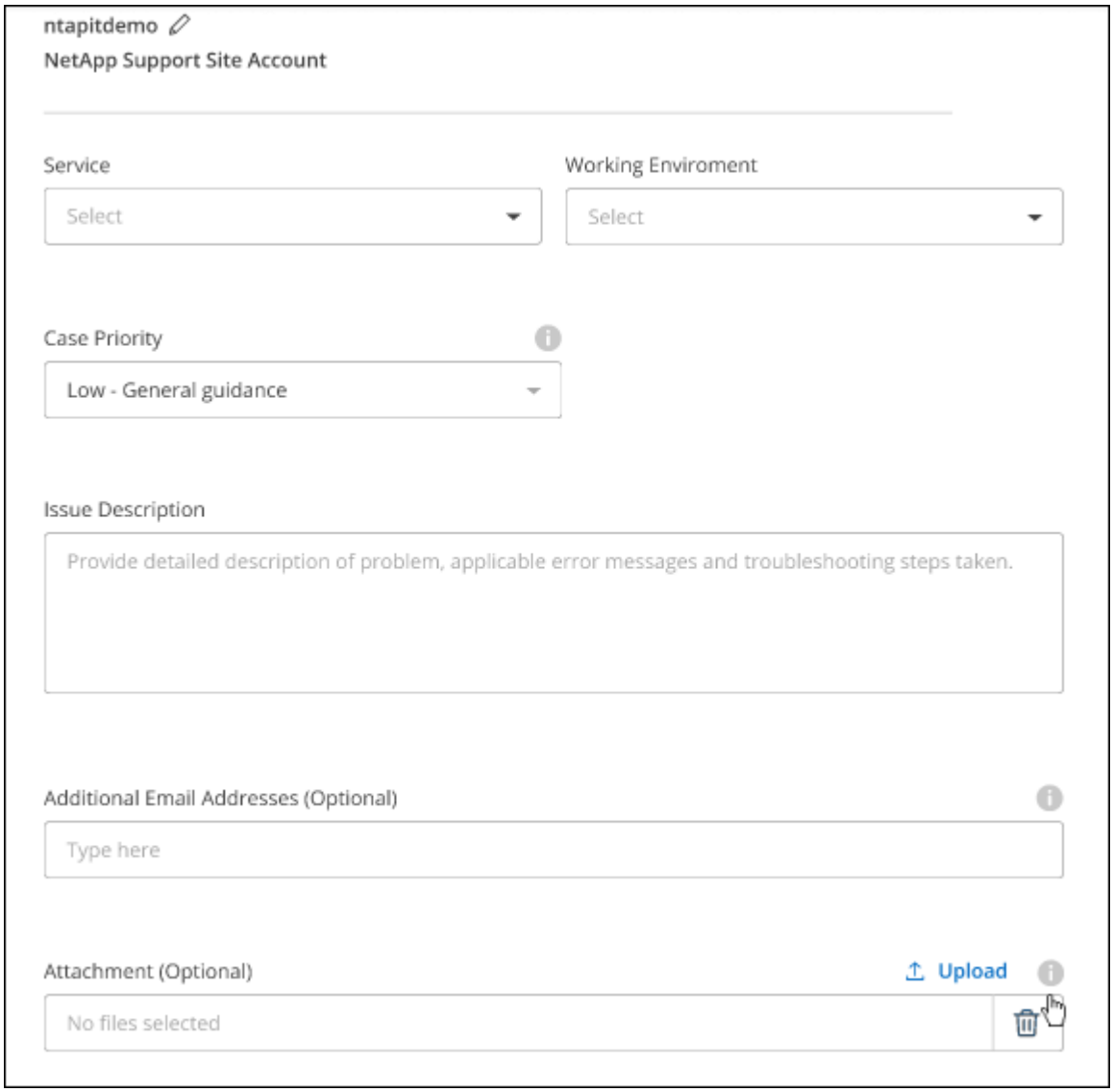
      - ケースの優先度：ケースの優先度を低、中、高、または緊急から選択します。

        これらの優先事項に関する詳細については、フィールド名の横にある情報アイコンにマウスカー

ソルを合わせてください。

- 事象の説明：問題の詳細な説明を、該当するエラーメッセージや実行したトラブルシューティング手順を含めて提供してください。
- 追加のメールアドレス：この問題について他の方にも通知したい場合は、追加のメールアドレスを入力してください。
- 添付ファイル（任意）：最大5つの添付ファイルを一度に1つずつアップロードできます。

  添付ファイルは1ファイルあたり25MBまでです。以下のファイル拡張子がサポートされています：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。



終了後の操作

サポートのケース番号が記載されたポップアップが表示されます。NetAppのサポート スペシャリストがお客様のケースを確認し、間もなくご連絡いたします。

サポートケースの履歴を確認するには、*設定 > タイムライン*を選択し、「サポートケースの作成」という名前のアクションを探してください。一番右にあるボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとした際に、以下のエラーメッセージが表示される場合があります。

「選択されたサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられている記録上の会社が、NetApp Console アカウントのシリアル番号（例：960xxxx）または作業環境のシリアル番号の記録上の会社と同じでないことを意味している可能性があります。次のいずれかの方法でサポートを受けることができます：

- 技術的な内容以外のケースを提出するには https://mysupport.netapp.com/site/help

サポートケースを管理する

コンソールから直接、アクティブなサポートケースと解決済みのサポートケースを表示および管理できます。NSSアカウントおよび所属企業に関連付けられた案件を管理できます。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、2つの表示方法があります。
  - 左側の画面には、ご提供いただいたユーザー NSS アカウントで過去 3 ヶ月間にオープンされた案件の総数が表示されます。
  - 右側の画面には、ユーザーのNSSアカウントに基づいて、過去3か月間に貴社レベルで開設されたケースの総数が表示されます。

  表に表示されている結果は、選択したビューに関連する事例を反映しています。
- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は、ソート機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- 案件ごとに、案件メモを更新したり、既に「クローズ済み」または「クローズ保留中」の状態になっていない案件をクローズしたりする機能を提供しています。

手順

1. NetApp Console で、 * ヘルプ > サポート * を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSSアカウントをNetApp Consoleに追加してください。

   *ケース管理*ページには、コンソールユーザーアカウントに関連付けられているNSSアカウントに関連する未解決のケースが表示されます。これは、*NSS管理*ページの最上部に表示されているNSSアカウントと同じものです。
3. テーブルに表示される情報を必要に応じて変更できます。
   - *組織のケース*の下にある*表示*を選択すると、貴社に関連付けられているすべてのケースが表示されます。
   - 日付範囲を変更するには、正確な日付範囲を選択するか、別の期間を選択してください。
   - 列の内容をフィルタリングします。
   - テーブルに表示される列を変更するには、  を選択してから、表示する列を選択します。

4. ...を選択し、利用可能なオプションのいずれかを選択して、既存のケースを管理します：
   - ケースを表示：特定のケースに関する詳細情報を表示します。
   - ケースメモの更新：問題に関する詳細情報を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付してください。

     添付ファイルは1ファイルあたり25MBまでです。以下のファイル拡張子がサポートされています：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。
   - ケースを閉じる：ケースを閉じる理由の詳細を入力し、*ケースを閉じる*を選択してください。

NetApp Console ローカル展開に関する法的通知

NetApp Console ローカルデプロイメントのドキュメント（このページ用）。

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルは、NetAppソフトウェアで使用されるサードパーティの著作権とライセンスに関する情報を提供します。

"NetApp Consoleに関する通知".

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権を有し、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権については、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。